GeoVision inc
The Vision of Security

GV-Manager

Manuel utilisateur V1.1

© 2008 GeoVision, Inc. Tous droits réservés.
Ce manuel est protégé par les lois de copyright et ne peut pas être copié, en partie ou en entier, sans la permission écrite de GeoVision.

Tous les efforts ont été fait pour assurer que le contenu de ce manuel est correct et à jour. GeoVision décline toute responsabilité en cas d'erreur typographique ou d'impression.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tél. : +886-2-8797-8377
Fax : +886-2-8797-8335
http://www.geovision.com.tw

Marques utilisées dans ce manuel : *GeoVision*, le logo *GeoVision* et la gamme de produits GV sont des marques déposées de GeoVision, Inc. *Windows* et *Windows XP* sont des marques commerciales déposées de Microsoft Corporation.

Juin 2008

Table des matières

Chapitre 1 Introduction 3
1.1 Caractéristiques principales 4
1.2 Concepts 5

Chapitre 2 Installation 7
2.1 Installation de ASManager 7
2.2 Connexion 8

Chapitre 3 L'écran principal de ASManager 9
3.1 Ecran principal 9
3.1.1 Barre d'outils 10
3.2 Visualisation des périphériques 11
3.2.1 Contrôles de la fenêtre 12
3.3 Fenêtres de surveillance 12
3.3.1 Contrôles de la fenêtre 13
3.3.2 Personnaliser une Fenêtre de surveillance 14
3.3.3 Arranger les Fenêtres de surveillance 15

Chapitre 4 Configuration 17
4.1 Organigramme de réglage 17
4.2 Ajouter des Contrôleurs 18
4.2.1 Etape 1 : Configuration d'un Contrôleur de porte 18
4.2.2 Etape 2 : Configuration d'une Porte 19
4.3 Réglage des Badges 21
4.3.1 Ajouter un seul badge 22
4.3.2 Ajouter un Groupe de badges 24
4.3.3 Importer/exporter les données des badges 24
4.4 Réglage des Plannings hebdomadaires 26
4.4.1 Etape 1 : Régler les plages horaires 26
4.4.2 Etape 2 : Réglage des Plannings hebdomadaires 28
4.4.3 Etape 3 : Réglage des Jours fériés 30
4.5 Réglage des Groupes d'accès 31
4.6 Réglage des Utilisateurs de badge 32
4.6.1 Ajouter un Utilisateur de carte 32
4.6.2 Assigner un Badge à un Utilisateur 33
4.6.3 Envoyer des alertes SMS 34
4.6.4 Personnaliser un champ de données 34
4.6.5 Importer/Exporter les données des utilisateurs de badge 35

Chapitre 5 Intégration vidéo 37
5.1 Mapping de caméras 37
5.2 Accéder à une Vue en direct 39
5.3 Accéder à une image vidéo 39
5.4 La fenêtre Multi-vue 40
5.4.1 Ajouter une Vue Matrice 41
5.5 Récupérer des vidéos enregistrées 42

Chapitre 6 ASLog 45

Chapitre 7 Autres fonctions 47
7.1 Configuration d'un utilisateur du système 47
7.1.1 Ajouter un nouvel utilisateur 47
7.1.2 Editer un utilisateur existant 49
7.1.3 Modifier le mot de passe lors de la connexion 49
7.2 Configuration de notification 50
7.2.1 Configuration du serveur SMS 50
7.2.2 Configuration du serveur email 51
7.2.3 Configuration des notifications 52
7.3 Configuration de démarrage et de sauvegarde 53

Chapitre 8 ASRemote 55
8.1 Installation de ASRemote 55
8.2 La fenêtre de ASRemote 56
8.2.1 Barre d'outils 57
8.3 Connexion à ASManager 58

Chapitre 9 ASWeb 61
9.1 Connexion à ASManager 61
9.2 Accéder aux journaux 63
9.2.1 Utilisation d'un critère de recherche 63
9.2.2 Icônes de la fenêtre de journal 64
9.2.3 Exporter des journaux 65
9.2.4 Définir des colonnes 65

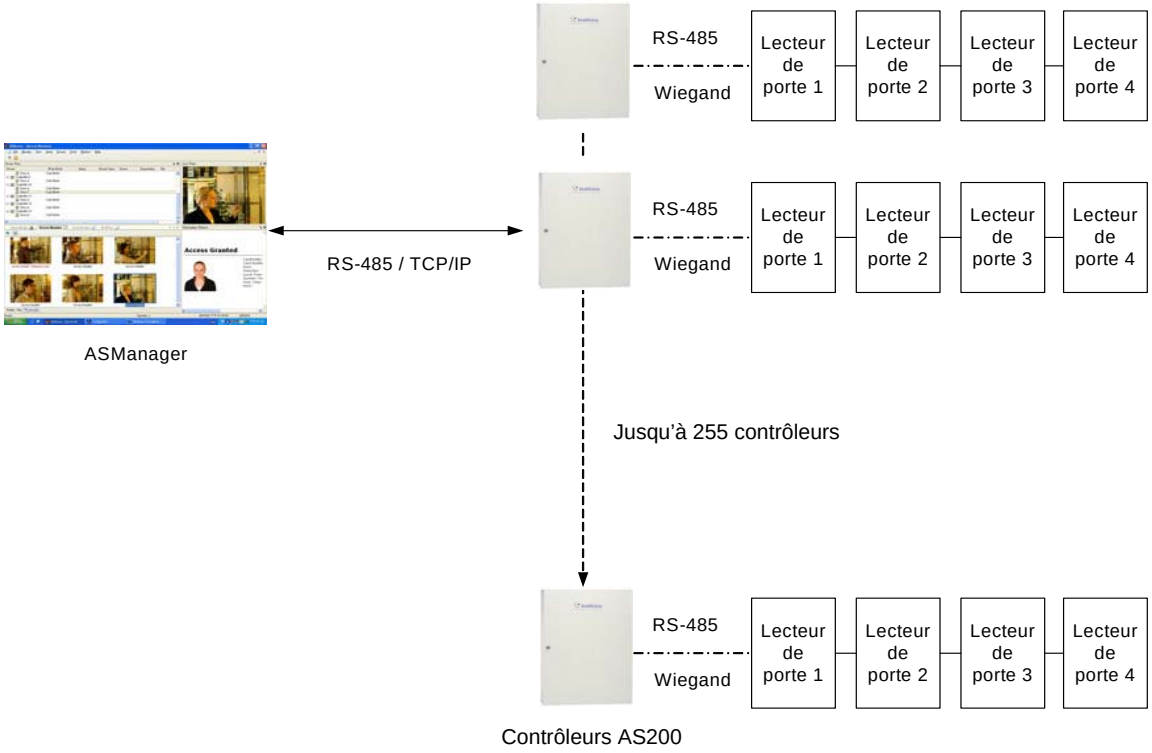
Chapitre 10 Guide de dépannage 67

Appendice 73
A. Appareils IP compatibles 73
B. Notifications d'événements 74
C. Symboles d'alerte Email et SMS 78

Chapitre 1 Introduction

ASManager et le Contrôleur AS200, lorsque utilisés ensemble, permettent de contrôler toutes les entrées de vos locaux. Vous pouvez surveiller et contrôler jusqu'à 255 Contrôleurs AS200 avec un ASManager.

Le diagramme suivant est un exemple illustrant comment ASManager et des Contrôleurs AS200 peuvent être installés.



1.1 Caractéristiques principales

ASManager

- Contrôle jusqu'à 255 Contrôleurs GV-AS
- Jusqu'à 256 plages horaires et plannings hebdomadaires
- Jusqu'à 10 000 badges
- Jusqu'à 1 000 utilisateurs du système
- Planning de vacance pour 14 mois
- Multiples badges par utilisateur
- Quatre (4) options de mode d'accès : Mode Badge seulement (Défaut), Mode Badge et code PIN, Mode Badge ou clavier numérique, Mode accès ouvert
- Mode Inscription des badges par lots
- Alarmes de porte : porte restée ouverte, entrée porte forcée, vandalisée, accès refusé
- Opération Contrainte
- Capacité Anti-passback
- Configuration sas avec deux portes
- Importer/exporter les badges et les données des utilisateurs de badge dans le format Access ou Excel
- Matrices définis par l'utilisateur avec multi-vues 16 canaux
- Mise en page d'écran définie par l'utilisateur et support d'affichage sur deux moniteurs
- Notification par SMS ou Email avec contenu défini par l'utilisateur, cliché vidéo et photo du porteur de badge
- Intégration vidéo avec les produits IP GeoVision (GV-System, GV-NVR, GV-Vidéo serveur, GV-Compact DVR, GV-IP caméra) et les caméras IP de tiers

ASLog

- Informations d'enregistrement avec vidéo et photo correspondant

ASRemote

- Surveille un nombre illimité de ASManager via Internet
- Surveillance de porte à distance, lecture vidéo, opération des portes

ASWeb

- Interface Web pour la recherche des informations d'enregistrement historiques avec vidéo et photo correspondant
- Export des journaux dans les formats Excel, Texte, HTML

1.2 Concepts

Il est important de comprendre les concepts suivants avant de continuer la lecture de ce manuel.

Planning hebdomadaire	Un planning hebdomadaire est certains jours de la semaine pendant lesquels peut avoir accès à site sécurisé. Pour plus de détails, voir *4.4 Réglage des Plannings hebdomadaires.*
Groupe d'accès	Un groupe d'accès est un groupe d'utilisateurs de badge avec des restrictions d'emplacement identiques et les mêmes contraintes de temps. Pour plus de détails, voir *4.5 Réglage des Groupes d'accès.*
Condition d'alarme	Une condition d'alarme est une condition qui est surveillée par des capteurs, et qui une condition d'alarme peut activer des alarmes. Le Contrôleur AS200 peut surveiller jusqu'à 3 capteurs, par exemple un capteur d'état de porte, un détecteur de fumée et un détecteur de vandalisme. Le Contrôleur AS200 possède aussi 3 relais de sortie pour activer et réactiver le verrouillage électrique, la sonnerie et l'ouverture d'urgence des portes lorsque la condition d'alarme se produit. Pour les réglages des conditions d'alarme, voir *4.2.2 Etape 2 : Configuration d'une porte*. Pour la configuration des entrées et des sorties, voir *Guide d'installation matérielle du Contrôleur AS200.*
Contrainte	Si une personne est forcée à ouvrir une porte sous contrainte, il peut entrer son PIN plus 1 pour activer une alarme et envoyer un signal à ASManager pour avertir la police. Par exemple, le code PIN est 5555 et vous entrez 5556. La porte s'ouvrira normalement (accès accordé) et l'alarme sera activée. Cette fonction est activée par défaut dans le système.
Anti-passback	Cette fonction est conçue pour éviter qu'un badge ne puisse être partagé et pour contraindre 0 une utilisation des lecteurs à des points d'entrée et de sortie. Lorsqu'un badge a été utilisé à un point d'entrée, il doit être utilisé à un point de sortie avant de pouvoir être réutilisé à un point d'entrée. Pour les réglages, voir *4.2.2 Etape 2 : Configuration d'une porte*.
Verrouillage	Cette fonction est aussi appelée un « sas » ou « verrouillage interdépendant ». Cette fonction contrôle deux portes en même temps et ne permet que l'ouverture d'une seule porte à tout moment. Cette fonction bloquera l'ouverture d'une porte si l'autre porte est déjà ouverte. Si les deux portes sont ouvertes en même temps, l'alarme s'activera. Pour les réglages, voir *4.2.1 Etape 1 : Configuration d'un Contrôleur de porte*.

Règle de double validation d'accès A/B	La porte ne s'ouvrira que lorsque les deux badges assignés à cette porte sont utilisés ensembles. Pour les réglages, voir *4.3.1 Ajouter un seul badge*.
Périphérique IP	La périphérique vidéo est connecté à ASManager via le réseau. ASManager vous permet d'accéder à la vidéo en direct aux produits IP de GeoVision (GV-System, GV-NVR, GV-Vidéo serveur, GV-Compact DVR, GV-IP caméra) et à certaines caméras IP de tiers. Pour plus de détails, voir *Intégration vidéo* dans Chapitre 5.

Chapitre 2 Installation

2.1 Installation de ASManager

Il est nécessaire d'utiliser un clé ''Dongle'' Keypro pour initialiser le programme ASManager. Les clé ''Dongle'' Keypros suivantes sont disponibles :

- **Keypro 4** est utilisé pour connecter jusqu'à 4 Contrôleurs AS200.
- **Keypro 10** est utilisé pour connecter jusqu'à 10 Contrôleurs AS200.
- **Keypro 30** est utilisé pour connecter jusqu'à 30 Contrôleurs AS200.
- **Keypro 50** est utilisé pour connecter jusqu'à 50 Contrôleurs AS200.
- **Keypro 255** est utilisé pour connecter jusqu'à 255 Contrôleurs AS200.

Configuration du système

Le disque dur de l'ordinateur où ASManager va être installé doit être : 2,4Go ou plus.

Pour installer les pilotes Keypro :

Insérez le CD du programme dans votre ordinateur ; une fenêtre s'affichera automatiquement. Choisissez **Install or Remove GeoVision GV-Series Driver (Installer ou désinstaller le pilote de la gamme GV GeoVision)** et cliquez sur **Install Geovision USB Devices Driver (Installer le pilote de périphériques USB Geovision)**.

Pour installer ASManager :

Insérez le CD du programme dans votre ordinateur ; une fenêtre s'affichera automatiquement. Choisissez **Install GeoVision V1.1 Access Control System (Installer le système de contrôle d'accès GeoVision V1.1)**, cliquez sur **GeoVision Access Control System (Système de contrôle d'accès GeoVision)** et suivez les instructions à l'écran pour terminer l'installation.

2.2 Connexion

Pour lancer ASManager, cliquez sur **Démarrer**, allez sur **Programmes**, choisissez **AS200** et cliquez sur **ASManager**. Lorsque vous lancez le système la première fois, le système vous demandera d'entrer l'Identifiant du superviseur et le Mot de passe, comme indiqué ci-dessous.

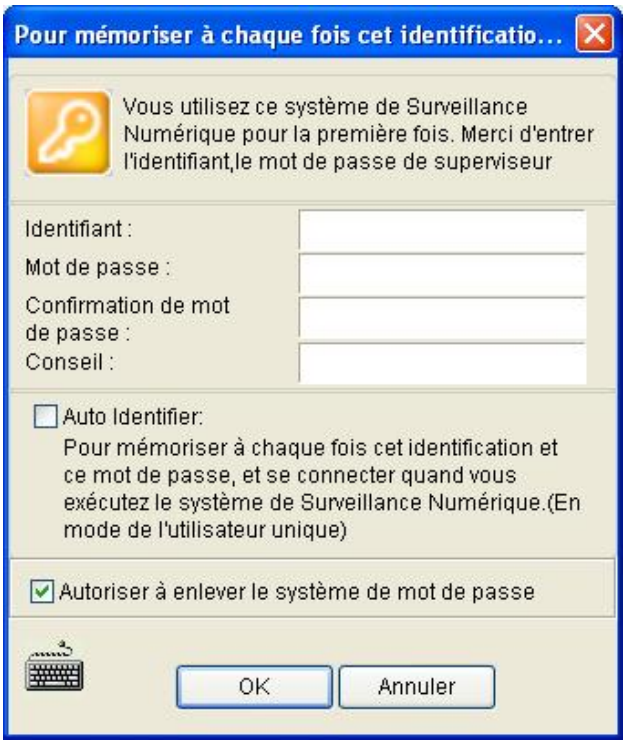

Pour mémoriser à chaque fois cet identificatio...
Vous utilisez ce système de Surveillance Numérique pour la première fois. Merci d'entrer l'identifiant,le mot de passe de superviseur
Identifiant :
Mot de passe :
Confirmation de mot de passe :
Conseil :
Auto Identifier:
Pour mémoriser à chaque fois cet identification et ce mot de passe, et se connecter quand vous exécutez le système de Surveillance Numérique.(En mode de l'utilisateur unique)
Autoriser à enlever le système de mot de passe
OK
Annuler

Figure 2-1

Entrez un nom de Superviseur dans le champ Identifiant. Terminez les réglages en entrant un Mot de passe, une Confirmation de mot de passe et un pense-bête (optionnel) pour vous aider si vous oubliez le mot de passe. Les options disponibles dans la boîte de dialogue sont :

- **Auto Identifiant :** Permet de vous connecter automatiquement avec cet identifiant chaque fois que le système est lancé. Pour des raisons de sécurité, cette option n'est recommandée qu'avec les systèmes où il n'y a qu'un seul utilisateur.
- **Autorisation d'enlever le système de mot de passe :** Permet à l'utilisateur d'effacer l'identifiant et le mot de passe de la base de données de système. Il est recommandé de cocher cette option en cas d'oubli du mot de passe. Pour plus de détails, voir la même option dans la Figure 7-1.
- **:** Cliquez sur cette icône pour afficher le clavier sur l'écran et entrer les informations de connexion.

Cliquez sur **OK** pour retourner à l'écran principal de ASManager.

Chapitre 3 L'écran principal de ASManager

Lorsque vous lancez ASManager, l'écran principal suivant s'affiche. Familiarisez-vous avec l'écran principal car cela sera utile au fur et à mesure que vous lisez les sections de ce manuel.

3.1 Ecran principal

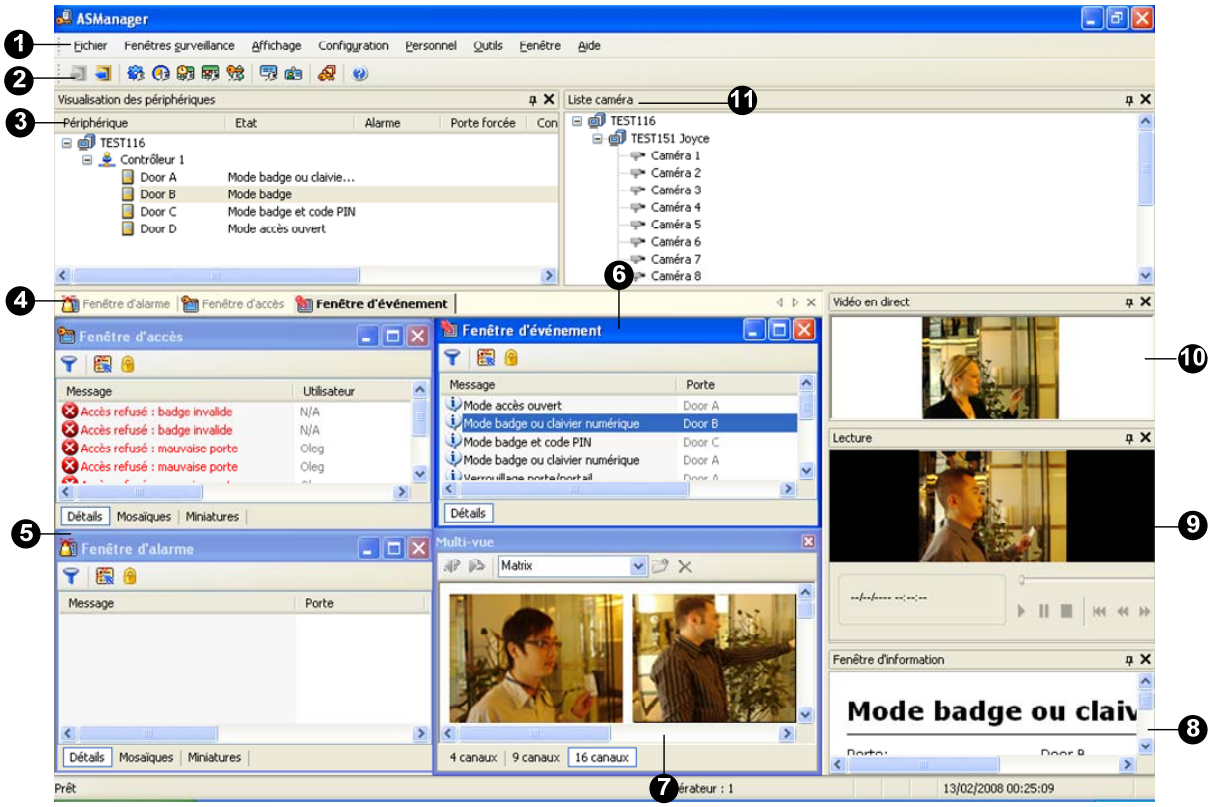


Figure 3-1

Nº	Nom	Fonction
1	Barre de menu	La Barre de menu permet d'accéder aux menus **Fichiers** (connexion/déconnexion à ASManager), **Fenêtres Surveillance** (afficher les fenêtres de surveillance des alarmes, des accès et des événements), **Affichage** (afficher les fenêtres de fonction), **Configuration** (Configurer les appareils connectés et les programmes), **Personnel** (configurer les comptes des utilisateurs de badge), **Outils** (configurer les notes et le journal) et **Fenêtre** (arranger l'affichage des différentes fenêtres).

2	Barre d'outils	La Barre d'outils contient les options **Connexion, Déconnexion, Périphériques, Plages horaires, Planning, Jours feriés, Groupes d'accès, Badges, Utilisateurs, ASLog** et **A propos de.**
3	Visualisation périphérique	Affiche une liste des portes connectées et leurs états.
4	Fenêtre d'événement	Affiche les événements surveillés des contrôleurs.
5	Fenêtre d'accès	Affiche les activités d'accès des contrôleurs.
6	Fenêtre d'alarme	Affiche les événements d'alarme des contrôleurs.
7	Multi-vue	Affiche les vues en direct des caméras connectées de multiples caméras IP. Pour plus de détails, voir « Fenêtre Multi-vue » dans Chapitre 5.
8	Fenêtre d'information	Affiche les informations des portes, des lecteurs de badge et des événements surveillés.
9	Lecture	Relit les événements enregistrés à partir d'un périphérique IP GeoVision compatible. Pour plus de détails, voir « Récupérer les vidéo enregistrées » dans Chapitre 5.
10	Vidéo en direct	Affiche la fenêtre de vue en direct d'une caméra connectée. Pour plus de détails, voir « Accéder à la vue en direct » dans le Chapitre 5.
11	Liste des caméras	Affiche une liste de toutes les caméras connectées.

3.1.1 Barre d'outils

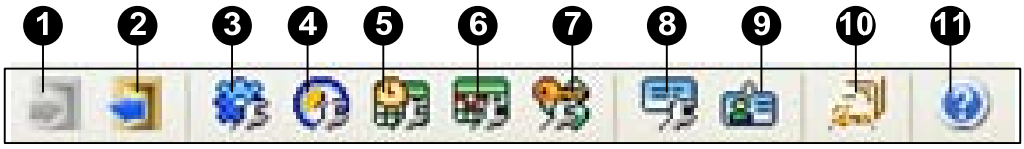


Figure 3-2

Les boutons de la Barre d'outils de ASManager :

Nº	Nom	Fonction
1	Connexion	Pour vous connecter à ASManager.
2	Déconnexion	Pour vous déconnecter de ASManager.
3	Périphériques	Pour définir les contrôleurs et les portes.

4	Plages horaires	Pour définir les heures et les minutes des jours pendant lesquels un utilisateur peut avoir accès à site sécurisé. Pour plus de détails, voir « Réglage des plages horaires » dans le Chapitre 4.
5	Plannings hebdomadaires	Pour définir les jours de la semaine pendant lesquels un utilisateur peut avoir accès à site sécurisé. Pour plus de détails, voir « Réglage des Plannings hebdomadaires» dans le Chapitre 4.
6	Jours fériés	Pour définir les dates des jours fériés. Pour plus de détails, voir « Réglage des Jours fériés » dans le Chapitre 4.
7	Groupes d'accès	Pour créer des groupes différents et définir chaque groupe d'accès à chaque porte à chaque moment de la journée. Pour plus de détails, voir « Réglage des Groupes d'accès » dans le Chapitre 4.
8	Badges	Pour créer et modifier une base de données des informations de badge. Pour plus de détails, voir « Réglage des Badges » dans le Chapitre 4.
9	Utilisateurs de badge	Pour créer et modifier une base de données des informations des utilisateurs de badge. Pour plus de détails, voir « Réglage des Utilisateurs de badge » dans le Chapitre 4.
10	ASLog	Affiche les journaux des activités d'accès, des rapports d'alarme et des événements surveillés. Pour plus de détails, voir Chapitre 6 *ASLog.*
11	A propos de	Affiche la version de ASManager.

3.2 Visualisation des périphériques

La fenêtre Visualisation périphérique affiche les activités et l'état des portes connectées.

- Pour ouvrir la fenêtre Visualisation des périphériques, cliquez sur **Affichage** dans la barre de menu et choisissez **Visualisation des périphériques**.

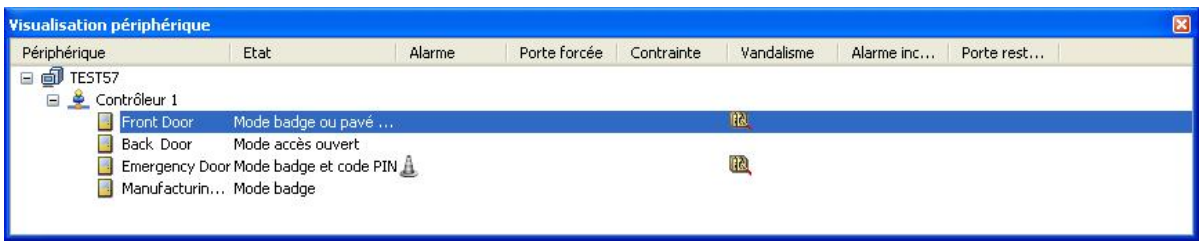


Figure 3-3

3.2.1 Contrôles de la fenêtre

Vous pouvez contrôler un contrôleur ou une porte connectée en cliquant sur le bouton droit dans la fenêtre Visualisation périphérique.

Les options du menu des contrôleurs sont les suivantes :

Nom	Fonction
Réinitialiser anti-passback	Cliquez sur cette option pour permettre à un utilisateur de réutiliser le lecteur d'un point d'entrée avant de sortir. Voir la fonction « Anti-Passback » dans Etape 2 dans la section 4.2.2 de *l'Etape 2: Configuration d'une porte*.
Mettre à jour	Une fois que les réglages d'un contrôleur ont été changé, cliquez sur Mise à jour pour utiliser immédiatement les nouveaux réglages.
Configuration	Utilisez la boîte de dialogue Configuration contrôleur pour changer les réglages d'un contrôleur.

Les options du menu des portes sont les suivantes :

Nom	Fonction
Déverrouiller la porte, Forcer le déverrouillage, Forcer le verrouillage et Désactiver verrouillage de la porte.	Contrôle l'état de la porte.
Effacer alarme, Effacer porte forcée, Effacer contrainte, Effacer vandalisme, Effacer alarme incendie, Effacer porte restée ouverte et Effacer accès refusé.	Efface les alarmes de la fenêtre Visualisation périphérique. Pour les réglages d'alarme, voir Etape 5 dans la section 4.2.2 de *Etape 2 : Configuration d'une porte.* Veuillez noter que Effacer alarme n'efface que les sons des alarmes.
Configuration	Utilisez la boîte de dialogue Configuration contrôleur pour changer les réglages d'un contrôleur.

3.3 Fenêtres de surveillance

Trois fenêtres de surveillance sont fournies pour permettre aux utilisateurs de surveiller différents types d'activités de porte : Fenêtre d'accès, Fenêtre d'alarme et Fenêtre d'événement.

- Pour ouvrir ces fenêtres, cliquez sur Fenêtre de **surveillance** dans la barre de menu et choisissez la fenêtre désirée.

3.3.1 Contrôles de la fenêtre

Les trois fenêtres de surveillance, Fenêtre d'accès, Fenêtre d'alarme et Fenêtre d'événement ont toutes les mêmes types de contrôle.

La Fenêtre d'accès est utilisée à titre d'exemple pour expliquer ces contrôles.

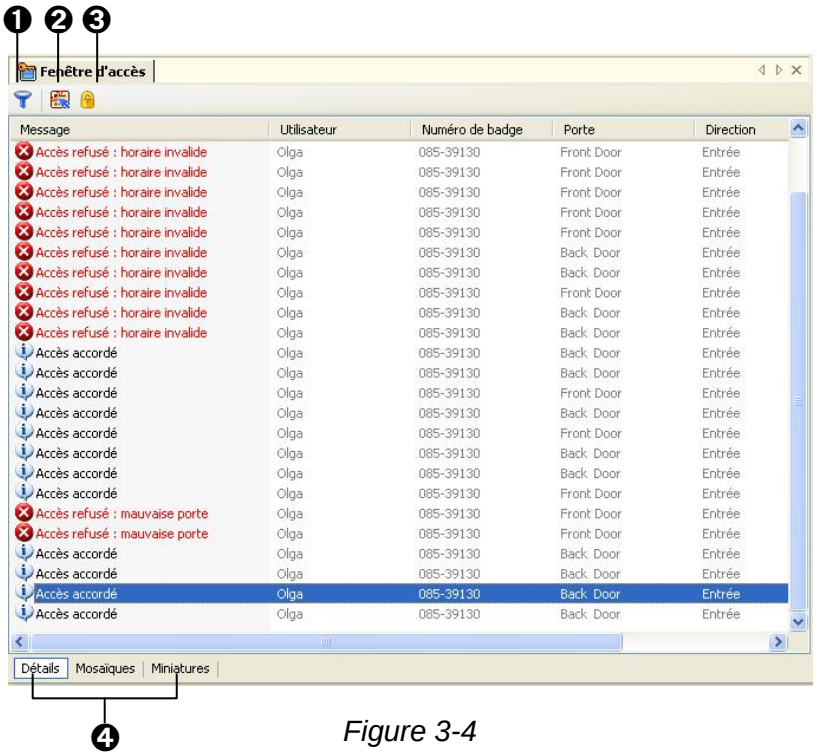


Figure 3-4

Nº	Nom	Fonction
1	Filtre	Pour choisir des critères et afficher seulement le type d'activité désiré.
2	Sélectionner automatiquement	Pour afficher seulement les dernières données.
3	Verrouillage	Pour suspendre l'affichage des données en cours.
4	Détails / Mosaïques / Miniatures	Pour choisir comment afficher les événements dans la fenêtre.

Lorsque vous cliquez à droite sur un message dans la fenêtre, un menu d'option s'affiche pour permettre d'accéder à des informations détaillées à propos du message.

- **Nouveau/Edition badge :** Pour créer un nouveau badge ou éditer les informations du badge.
- **Consulter les informations Badge :** Pour afficher les informations du badge.
- **Consulter les informations utilisateur :** Pour afficher les informations de l'utilisateur du badge.
- **Afficher l'image :** Si la caméra était en train d'enregistrer lorsque l'activité s'est produite, l'image correspondante est disponible.

3.3.2 Personnaliser une Fenêtre de surveillance

Vous pouvez personnaliser les messages affichés dans la fenêtre de surveillance en utilisant des critères de filtre : Vous pouvez ainsi ajouter des fenêtres personnalisées multiples en fonction de vos besoins.

1. Pour ajouter une fenêtre de surveillance, cliquez sur Fenêtre **surveillance** dans la bare de menu. Choisissez ensuite **Nouvelle fenêtre d'alarme**, **Nouvelle fenêtre d'accès** ou **Nouvelle fenêtre d'événement**.
2. Cliquez sur le bouton **Filtre** dans la fenêtre Surveillance. La boîte de dialogue suivante s'affiche.

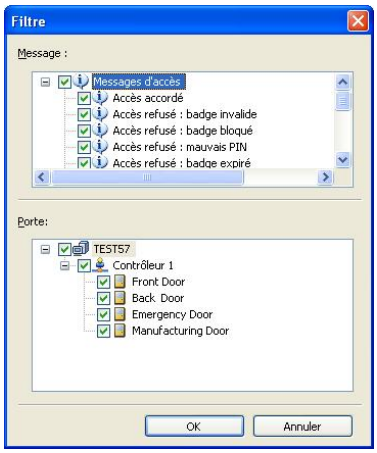


Figure 3-5

3. Choisissez les messages désirés et les périphériques de surveillance puis cliquez sur **OK**. Seulement les messages basés sur le critère défini s'afficheront dans la fenêtre de surveillance.
4. Cliquez à droite sur l'onglet Fenêtre dans l'écran principal et choisissez **Renommer** pour donner un nom à la nouvelle fenêtre de surveillance.

Figure 3-6

Remarque : Les fenêtres ajoutées ne seront utilisées qu'une seule fois et ne seront pas sauvegardées lorsque vous fermez ASManager.

3.3.3 Arranger les Fenêtres de surveillance

Les Fenêtres de surveillance peuvent être arrangées sur l’écran de plusieurs manières.

Dans la barre de menu, cliquez sur **Fenêtre** et choisissez l’une des options suivantes pour réarranger automatiquement les fenêtres :

- **Cascade :** Pour recouvrir partiellement les fenêtres ouvertes et afficher les barres de titre.
- **Mosaïque horizontale :** Pour arranger les fenêtres ouvertes horizontalement.
- **Mosaïque verticale :** Pour arranger les fenêtres ouvertes verticalement.
- **Arranger les icônes :** Pour arranger les fenêtres réduites en bas.

Si vous avez configuré plusieurs fenêtres de surveillance, vous pouvez aussi cliquer sur **Fenêtre** et choisir **Plus de fenêtres** pour voir la liste complète de toutes les fenêtres de surveillance.

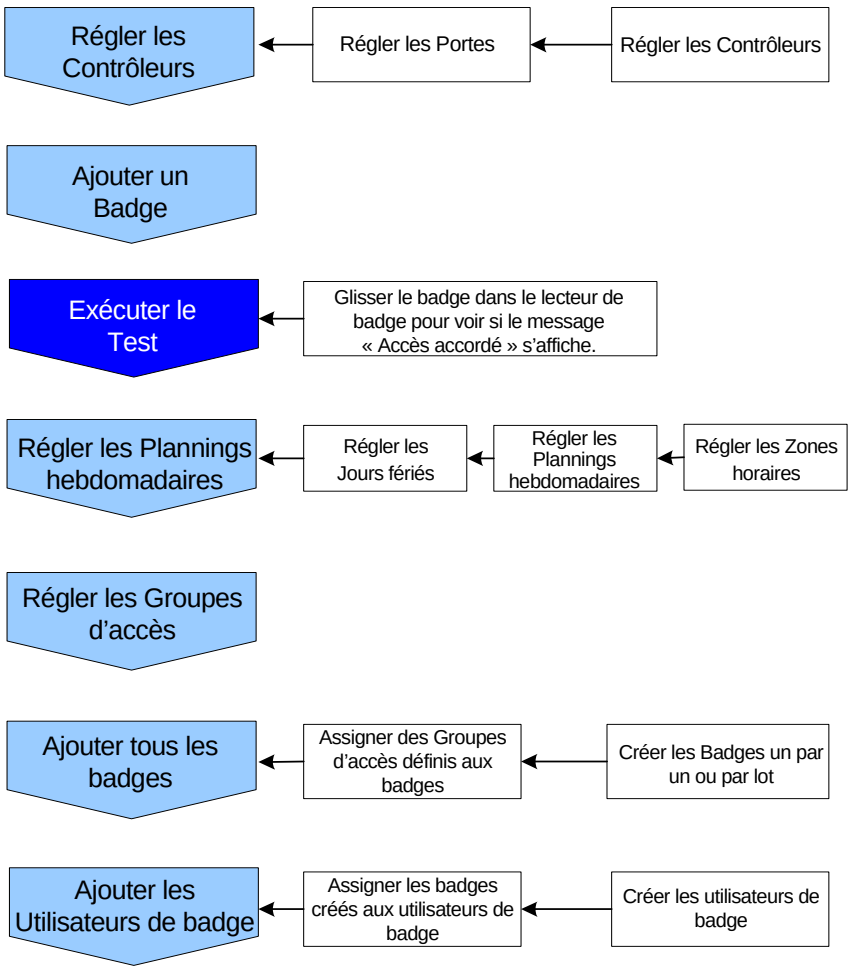
Chapitre 4 Configuration

Ce chapitre décrit les réglages suivants :

- Réglage des Contrôleurs
- Réglage des Badges
- Réglage des Plannings hebdomadaires
- Réglage des Groupes d'accès
- Réglage des Utilisateurs de badge

4.1 Organigramme de réglage

Pour vous aider avec les réglages de ASManager, suivez la méthode illustrée ci-dessous.


Régler les Contrôleurs
Régler les Portes
Régler les Contrôleurs
Ajouter un Badge
Exécuter le Test
Glisser le badge dans le lecteur de badge pour voir si le message « Accès accordé » s'affiche.
Régler les Plannings hebdomadaires
Régler les Jours fériés
Régler les Plannings hebdomadaires
Régler les Zones horaires
Régler les Groupes d'accès
Ajouter tous les badges
Assigner des Groupes d'accès définis aux badges
Créer les Badges un par un ou par lot
Ajouter les Utilisateurs de badge
Assigner les badges créés aux utilisateurs de badge
Créer les utilisateurs de badge

4.2 Ajouter des Contrôleurs

Pour ajouter le Contrôleur AS200 au ASManager, suivez les étapes suivantes :

- **Etape 1 Configuration d'un Contrôleur de porte**
  Etablissez la communication entre le Contrôleur AS200 et ASManager.
- **Etape 2 Configuration d'une Porte**
  Définissez les portes sur un contrôleur de porte.

4.2.1 Etape 1 : Configuration d'un Contrôleur de porte

1. Dans la barre de menu, cliquez sur **Configuration** et choisissez **Périphérique**. La boîte de dialogue Liste contrôleur s'affiche.
2. Cliquez sur l'icône **Ajouter** en haut à gauche. La boîte de dialogue suivante s'affiche.

Figure 4-1

3. Choisissez un **Identifiant** et un **Nom** pour le Contrôleur AS200 et cliquez sur **OK**. La boîte de dialogue suivante s'affiche.

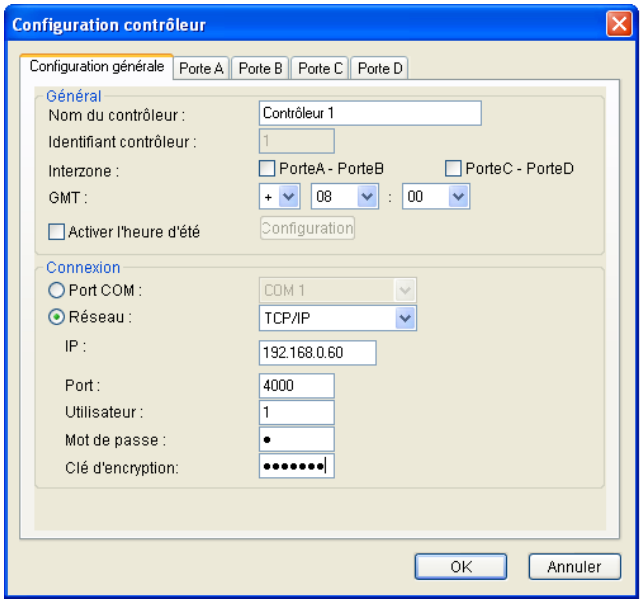


Figure 4-2

Remarque : Le Contrôleur d'ID AS200 est réglé en utilisant ASKeypad ou l'interface de configuration Web. Voir les sections « 5.2 Réglage des paramètres » et « 6.2.4 Réglage de l'Identifiant du Contrôleur et du Mode de fonctionnement » dans le *Guide d'installation matérielle du Contrôleur AS200*.

---

4. Dans la section Connexion, choisissez le mode de communication entre le Contrôleur AS200 et ASManager.
   - Si vous utilisez une connexion RS-485, choisissez le **Port COM** utilisé pour la connexion.
   - Si vous utilisez Ethernet, choisissez **Réseau** et sélectionnez **TCP/IP** ou **DDNS local**. Entrez l'adresse IP, le nom du périphérique (si DDNS local a été choisi), le numéro du port, l'identifiant de l'utilisateur, le mot de passe de l'utilisateur et la clé d'encryption (code 3DES) du contrôleur AS200.
5. Réglages OPTIONNELS de la section Général :
   - **Interzone :** Pour activer la fonction « verrouillage interdépendant » entre deux portes (Porte A et Porte B, ou Porte C et Porte D). Les portes qui sont verrouillées de cette manière ne peuvent pas être ouverte en même temps. Une porte est déverrouillée lorsque l'autre porte est fermée.
   - **GMT :** L'heure locale sur l'ordinateur hôte.
   - **Activer l'heure d'été :** Pour activer la fonction Heure d'été. L'heure du système changera automatiquement pour suivre l'heure d'été.

Remarque : Les réglages par défaut du Contrôleur AS200 sont : Adresse IP **192.168.0.100** ; nom d'utilisateur **admin**; mot de passe **1234**; clé d'encryption (code 3DES) **12345678**. Pour plus de détails sur les réglages du Contrôleur AS200, voir *Guide d'installation matérielle du Contrôleur AS200*.

4.2.2 Etape 2 : Configuration d'une Porte

1. Pour définir les portes d'un contrôleur, cliquez sur un onglet **Porte** (Porte A, Porte B, Porte C ou Porte D). La boîte de dialogue suivante s'affiche.

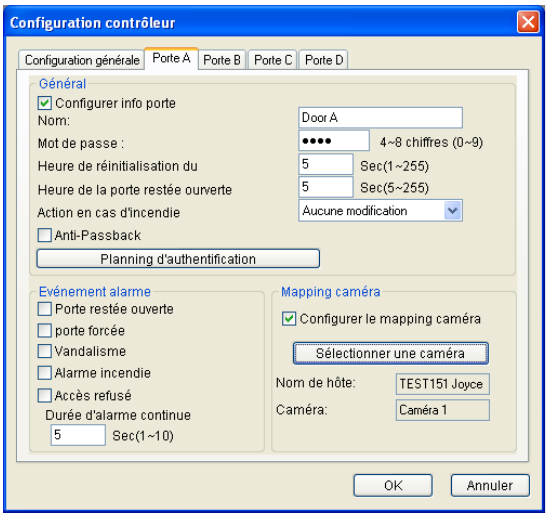


Figure 4-3

2. Dans la section Général, cochez l'option **Configuration info porte** pour définir les paramètres généraux de la porte :

   - **Nom :** Entrez le nom de la porte.
   - **Mot de passe :** Entrez le mot de passe de la porte. Le réglage par défaut est 1234.
   - **Heure de réinitialiser le verrouillage de la porte :** Si la porte est surveillée, entrez le nombre de secondes que la porte peut rester ouverte. Après cette durée de temps, la porte se verrouillera automatiquement.
   - **Temps d'alerte en cas de porte :** Si la porte est surveillée, entrez le nombre de secondes que la porte peut rester ouverte avant qu'une alarme de porte ouverte ne soit déclenchée.
   - **Action en cas d'incendie :** Réglez la porte sur verrouillé ou déverrouillé lorsqu'une condition d'alarme d'incendie se produit.
   - **Anti-Passback :** Lorsque l'option Anti-Passback est cochée, un badge utilisé pour ouvrir une porte d'entrée ne peut pas être réutilisé sur la même porte sans avoir en premier été utilisé pour ouvrir la porte de sortie correspondante. Ceci peut être utilisé avec les modes **Circulation à sens unique** et **Contrôle dans les deux sens**.

3. Pour définir le mode d'accès, cliquez sur le bouton **Planning**. La boîte de dialogue suivante s'affiche.

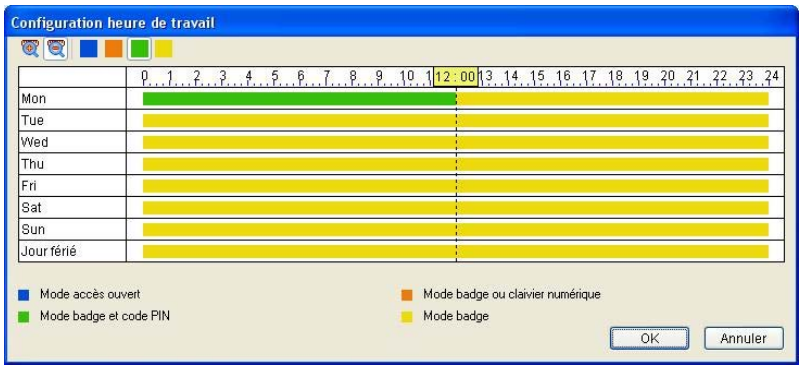


Figure 4-4

4. Pour définir quel type de mode d'accès doit être utilisé à certaines heures et jours, choisissez un mode d'accès dans la barre d'outils et faites glisser la souris sur les périodes désirées. Quatre (4) modes d'accès sont disponibles dans le système :

   - **Mode badge :** Ce mode est le mode par défaut. Ce mode exige que l'utilisateur glisse son badge pour ouvrir la porte.
   - **Mode accès ouvert :** Garde la porte dans un état ouvert avec le lecteur.
   - **Mode badge et code PIN :** Ce mode exige que l'utilisateur glisse son badge puis entre le code PIN du badge avec le pavé numérique.

- **Mode badge ou clavier numérique :** Ce mode exige que l'utilisateur présente son badge **OU** entre le mot de passe de la porte en utilisant le clavier numérique pour ouvrir la porte.

5. Les réglages de la section Evénement alarme sont OPTIONNELS sauf si un périphérique d'alarme est installé sur le Contrôleur AS200. Cochez les conditions d'alarme désirées qui causeront une activation de l'alarme. **Porte restée ouverte**, **Entrée forcée**, **Incendie**, **Le lecteur de carte est en train d'être vandalisé** et **Badge inconnu**.

   - **Durée d'alarme continue :** Entrez la durée de l'alarme, en secondes.

6. Les réglages de la section Mapping caméra sont OPTIONNELS sauf si une caméra a été installé dans un site sécurisé. Pour plus de détails, voir *Chapitre 5 Intégration vidéo.*

7. Cliquez plusieurs fois sur **OK** pour retourner à l'écran principal. Une liste de dossiers de contrôleur s'affichera dans la fenêtre Visualisation périphérique comme indiqué ci-dessous.

   Si l'icône est affichée, cela indique que la connexion entre le contrôleur et ASManager a été établie.

   Si l'icône est affichée, cela indique que la connexion a échoué. Assurez-vous que les réglages de la connexion sont correctement faits.

Figure 4-5

4.3 Réglage des Badges

Une fois que vous avez configuré l'unité de contrôle d'accès, vous pouvez commencer à enregistrer des badges. Tous les nouveaux badges doivent être enregistrés dans ASManager avant de pouvoir être utilisés pour avoir accès. Vous pouvez enregistrer jusqu'à 10 000 badges dans ASManager. Si un badge qui n'a pas été enregistré est utilisé dans un lecteur de badge, le message *Accès refusé : badge invalide* s'affichera.

En fonction du nombre de badges que vous voulez enregistrer, vous pouvez les ajouter un par un ou utiliser la fonction de lot pour ajouter un groupe de badges.

4.3.1 Ajouter un seul badge

1. Pour ajouter un badge, utilisez l'une des méthodes suivantes :

   - Faites glisser le badge dans le lecteur. le message Accès refusé : *badge invalid)* s'affichera. Cliquez avec le bouton droit sur le message et choisissez **Nouveau/Edition le badge**. la boîte de dialogue Nouveau badge s'affichera avec le numéro du badge et le code entré (voir Figure 4-7). Suivez l'étape 3 pour terminer les autres réglages.

   - Dans la barre de menu, cliquez sur **Personnel** et choisissez **Badges**. La fenêtre suivante s'affiche.

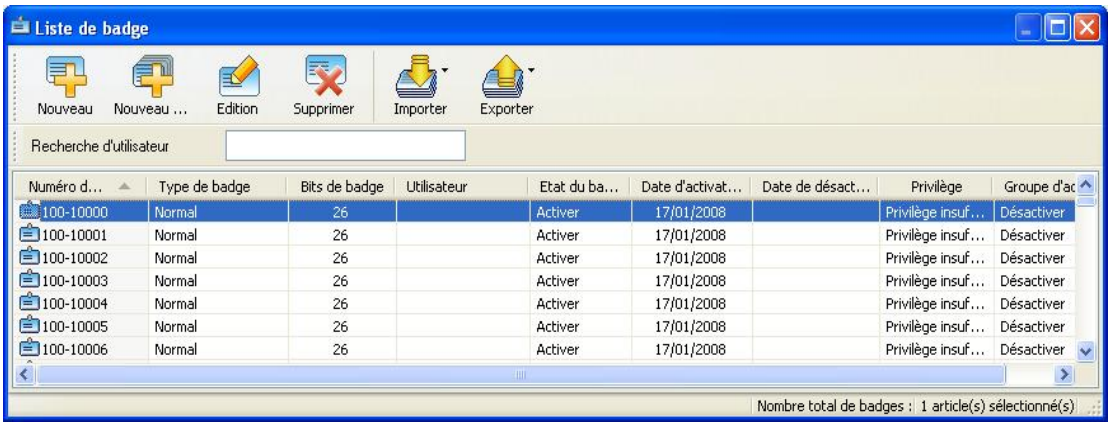


Figure 4-6

2. Cliquez sur le bouton **Nouveau** dans la barre d'outils. La boîte de dialogue suivante s'affiche.

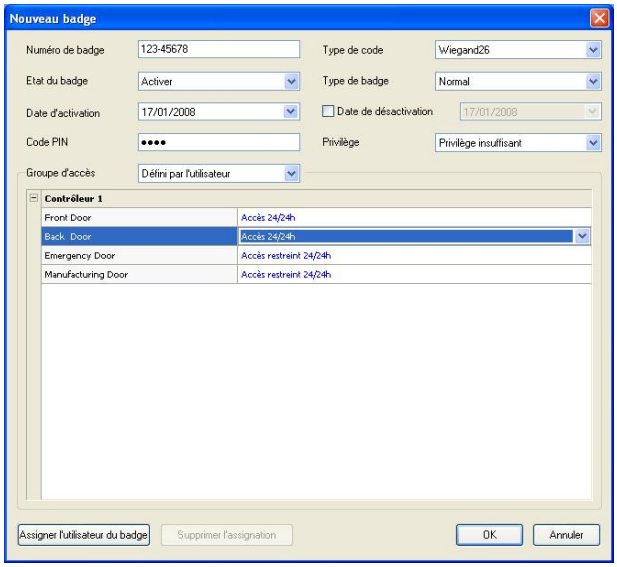


Figure 4-7

3. Les réglages disponibles pour le badge sont :

   - **Numéro de badge :** Entrez le numéro du badge.

- **Type de code :** Choisissez le format du badge.
- **Type de badge :**
  - **Patrouille :** Le badge est assigné à la personne responsable de patrouiller un endroit spécifique, par exemple un garde. Lorsque le badge de type Patrouille est utilisé avec le lecteur, l'accès sera enregistré et la porte ne se déverrouillera PAS. Cette fonction peut être utilisée avec **Privilège** ci-dessous. L'utilisateur peut avoir le droit d'arrêter les sons d'alarmes et d'effacer les alarmes pendant les patrouilles.
  - **Badge A : mode double présentation :** Règle de double présentation A/B. Le badge est défini comme Badge A et l'autre Badge B doit être utilisé en même temps pour déverrouiller les portes avec la règle de double présentation.
  - **Badge B : mode double présentation :** Règle de double présentation A/B. Le badge est défini comme Badge B et l'autre Badge A doit être utilisé en même temps pour déverrouiller les portes avec la règle de double présentation.
- **Date d'activation / Date de désactivation :** Pour spécifier lorsque le badge est actif ou inactif.
- **Code PIN :** Entrez un code personnel à 4 chiffres pour le badge. Le réglage par défaut est 1234.
- **Privilège :** Pour assigner un des privilèges suivants à l'utilisateur du badge :
  - **Arrêter l'alarme :** L'utilisateur du badge peut arrêter les sons d'alarme en utilisant le badge.
  - **Supprimer l'événement :** L'utilisateur du badge peut effacer les alarmes en utilisant le badge. Toutes les alarmes dans la fenêtre Visualisation périphérique seront effacées. Un enregistrement de ces alarmes est gardé dans Moniteur d'alarme.
- **Groupe d'accès :** Les Groupes d'accès contrôle qui peut ouvrir quelle porte à quelle heure. Pour plus de détails, voir *4.5 Réglage des Groupes d'accès.*

  Si vous utilisez ASManager la première fois, les groupes d'accès ne sont pas encore définis. Choisissez **Défini par l'utilisateur** pour faire un test de fonctionnement.
- **Contrôleur :** La colonne Contrôleur affiche les portes associés. La sélection pour chaque porte s'affichera automatiquement lorsqu'un groupe d'accès a été ouvert.

  Si vous utilisez ASManagerla première fois, choisissez **Accès 24/24h** pour chaque porte pour faire un test de fonctionnement.

4. Présentez la carte enregistrée au lecteur. Une fois que la carte a été acceptée, le message *Accès accordé* s'affichera.

4.3.2 Ajouter un Groupe de badges

Avant d'utiliser la fonction Lot pour enregistrer des nouveaux badges, veuillez noter que le groupe de badges doit être numéroté dans l'ordre.

1. Dans la barre de menu, cliquez sur **Personnel** et choisissez **Badges**. La boîte de dialogue Liste de badges s'affiche.
2. Cliquez sur le bouton **Nouveaux badges par lots** dans la barre d'outils. La boîte de dialogue suivante s'affiche.

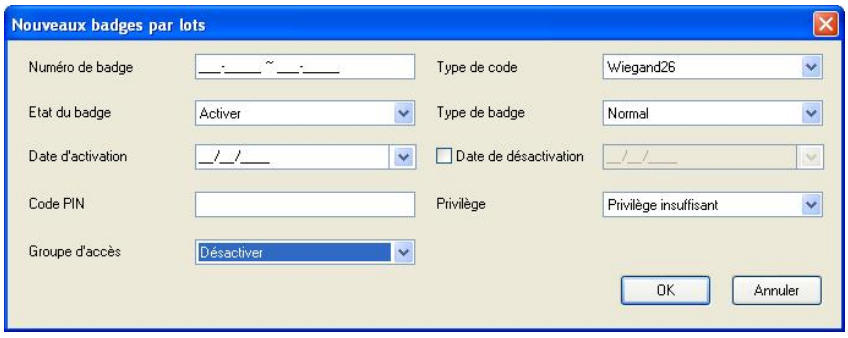


Figure 4-8

3. Les réglages de cette boîte de dialogue sont les mêmes que ceux pour ajouter un seul badge. Voir *Ajouter un seul badge*.

Remarque : Les badges qui ont été enregistrés en utilisant la fonction Lot auront tous le même PIN. Si vous voulez changer le PIN de certains badges, vous devez entrer le PIN en utilisant la fonction **Edition** de la boîte de dialogue Liste de badge.

4.3.3 Importer/exporter les données des badges

Vous pouvez importer et exporter les données des badges aux formats mdb et xls.

Pour exporter les données des badges :

1. Dans la fenêtre Liste de badge (voir Figure 4-6), choisissez les badges désirés avec Ctrl + clic gauche.
2. Cliquez sur le bouton **Exporter** et choisissez l'une des options suivantes : **Exporter vers Access** ou **Exporter vers Excel**.
3. Assignez le chemin de fichier et entrez un mot de passe optionnel pour exporter les données des badges.

Remarque : Le format de fichier Excel ne supporte pas la protection par mot de passe.

Pour importer les données des badges :

1. Dans la fenêtre Liste de badge (voir Figure 4-6), cliquez sur le bouton **Importer** et choisissez l'une des options suivantes : **Importer de Access** ou **Importer de Excel**.
2. Choisissez un chemin de fichier et entrez un **Mot de passe** si besoin. Cliquez sur **OK**. La boîte de dialogue suivante s'affiche.

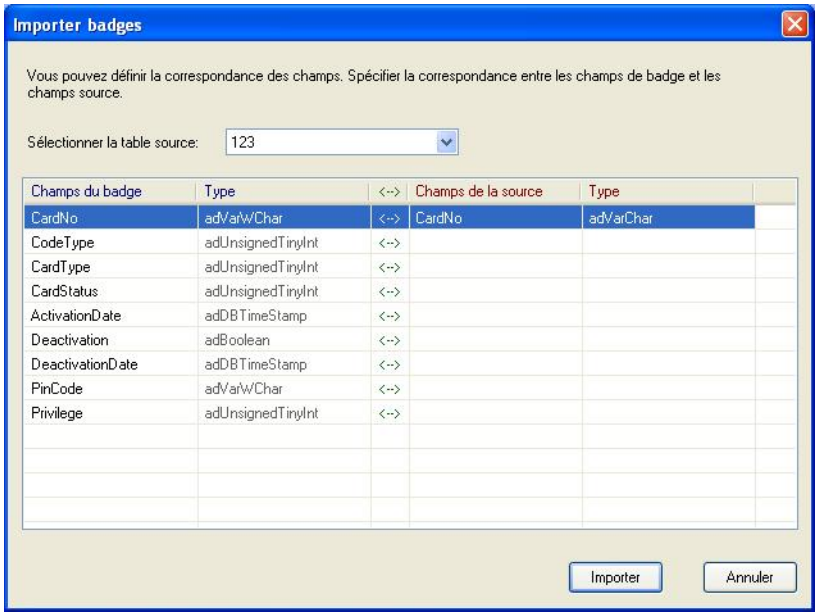


Figure 4-9

3. Sélectionnez la **Table source** désirée et cliquez sur les colonnes sous **Champs de la source** pour activer la sélection. Choisissez les éléments de source correspondants pour mapper entre Champs de la source et Champs du badge.
4. Cliquez sur **Importer** pour importer les données du badge.

4.4 Réglage des Plannings hebdomadaires

Cette section vous aidera à régler les temps d'accès journaliers et pendant les jours fériés. Vous pouvez définir jusqu'à 254 plannings hebdomadaires avec deux plannings hebdomadaires par défaut pour « accès refusé » et « accès autorisé ».

Avant de créer des plannings hebdomadaires, il est utile de décider en avance tous les plannings hebdomadaires possibles pour le site. Par exemple : Prenez en compte les différents horaires et les besoins des différents employés, par exemple, prenez en compte le personnel de nettoyage et d'entretien qui peut avoir besoin d'un accès la nuit, prenez en compte le personnel de maintenance ou de réparation qui peut avoir besoin d'un accès 24/24h, prenez en compte les superviseurs qui peuvent avoir besoin d'un accès le soir, etc.

- **Etape 1 Réglage des plages horaires**

  Pour définir les heures et les minutes des jours pendant lesquels un utilisateur peut avoir accès à site sécurisé. La durée minimum est de 5 minutes.

- **Etape 2 Réglage des Plannings hebdomadaires**

  Pour définir les jours de la semaine pendant lesquels un utilisateur peut avoir accès à site sécurisé.

- **Etape 3 Réglage des Jours fériés**

  Pour définir les dates des jours fériés.

4.4.1 Etape 1 : Régler les plages horaires

Cette section contient des exemples de réglage pour les plages horaires suivantes :

- Poste de jour – 09:00 à 19:00 heures
- Poste de nuit – 19:00 à 9:00 heures (sur minuit)
- Superviseur – 07:00 à 24:00 heures

1. Dans la barre de menu, cliquez sur **Configuration** et choisissez **Plages horaires**. La boîte de dialogue suivante s'affiche.

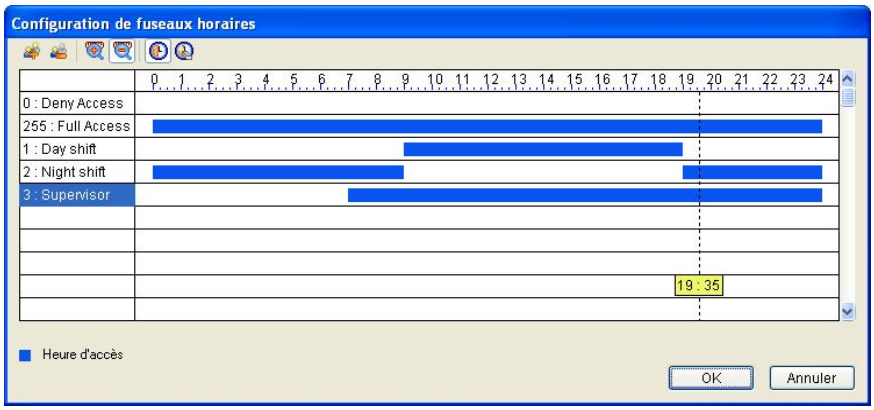

Configuration de fuseaux horaires
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
0 : Deny Access
255 : Full Access
1 : Day shift
2 : Night shift
3 : Supervisor
19 : 35
Heure d'accès
OK
Annuler

Figure 4-10

2. Cliquez sur le bouton **Ajouter** . La boîte de dialogue suivante s'affiche.

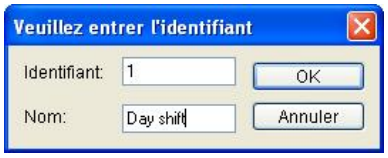


Figure 4-11

3. L'**Identifiant** est le numéro de la plages horaire. Le système va automatiquement créer l'identifiant en fonction du nombre de plages horaires créées. Entrez un **Nom** pour la plage horaire que vous allez définir. Cliquez sur **OK**.

   Par exemple, appelez la plages horaire 1 **day shift (Poste de jour)**.

4. Cliquez sur le bouton **Ajouter heure d'accès** . Puis glissez la souris sur les heures désirées pour définir la période de temps d'accès.

   Par exemple, les heures du poste de jour sont **de 09:00 à 19:00**.

5. Pour créer une deuxième plage horaire, cliquez sur le bouton **Ajouter** et entrez le nom **night shift (Poste de nuit)**. Puis cliquez sur le bouton **Ajouter heure d'accès**. Glissez la souris sur la barre de temps pour régler l'heure **de 19:00 à 24:00 et de 00:00 à 09:00**.

6. Pour créer une troisième plage horaire, cliquez sur le bouton **Ajouter** et entrez le nom **Superviseur**. Puis cliquez sur le bouton **Ajouter heure d'accès**. Glissez la souris sur la barre de temps pour régler l'heure **de 07:00 à 24:00**.

7. Cliquez sur **OK**. Les trois plages horaires ont été définies.

4.4.2 Etape 2 : Réglage des Plannings hebdomadaires

Cette section contient des exemples de réglage pour les plannings hebdomadaires suivants :

- Planning - Poste de jour – Lundi à Vendredi, 09:00 à 19:00 heures
- Planning - Poste de nuit – Lundi à Vendredi, 19:00:00 à 9:00 heures
- Planning - Superviseur – Lundi à Dimanche et Jours fériés, 07:00 à 24:00 heures

1. Dans la barre de menu, cliquez sur **Configuration** et choisissez **Plannings hebdomadaire**. La boîte de dialogue suivante s'affiche.

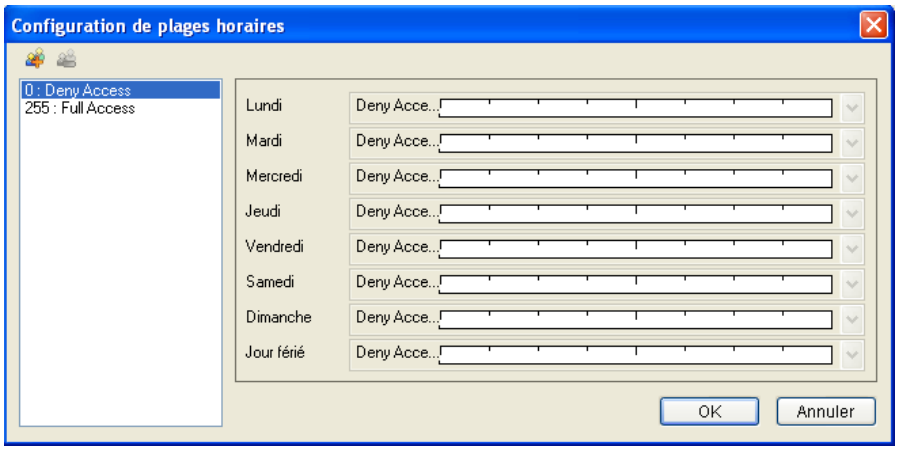


Figure 4-12

2. Cliquez sur le bouton **Ajouter**. La boîte de dialogue suivante s'affiche.

Figure 4-13

3. L'**Identifiant** est le numéro du planning hebdomadaire. Le système va automatiquement créer l'identifiant en fonction du nombre de plannings créés. Entrez un **Nom** pour le planning hebdomadaire que vous allez définir. Cliquez sur **OK**.

   Par exemple, appelez le Planning hebdomadaire 1 **Planning - Poste de jour**.

4. Dans la liste déroulante de **Lundi** à **Vendredi**, choisissez la plage horaire **Poste de jour** que nous avons créé. Aucun accès ne sera permis Samedi, Dimanche et pendant les jours fériés.

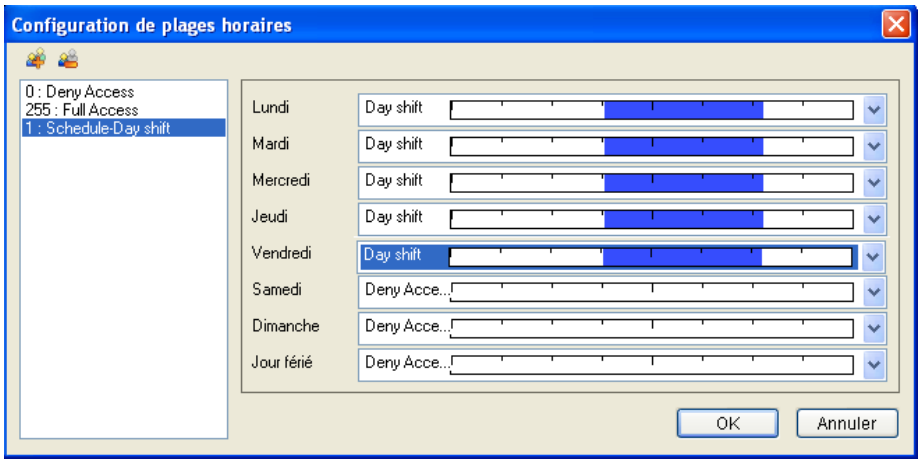


Figure 4-14

5. Pour créer un deuxième planning, cliquez sur le bouton **Ajouter** et entrez le nom **Planning - Poste de nuit**. Dans la liste déroulante de **Lundi** à **Vendredi**, choisissez la plage horaire **Poste de nuit** que nous avons créé. Aucun accès ne sera permis Samedi, Dimanche et pendant les jours fériés.

6. Pour créer un troisième planning, cliquez sur le bouton **Ajouter** et entrez le nom **Planning – Superviseur**. Dans la liste déroulante de **Lundi** à **Jours férié**, choisissez la plage horaire **Superviseur (Supervisor)** que nous avons créé.

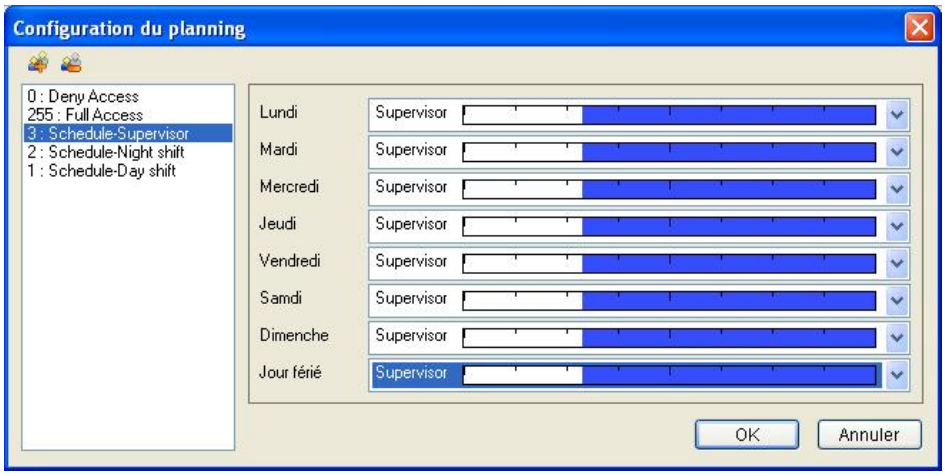


Figure 4-15

7. Cliquez sur **OK**. Les trois plannings hebdomadaires ont été définis.

4.4.3 Etape 3 : Réglage des Jours fériés

Pour définir certaines dates comme des jours fériés sur le système :

1. Dans la barre de menu, cliquez sur **Configuration** et choisissez **Jours fériés**. La boîte de dialogue suivante s'affiche.

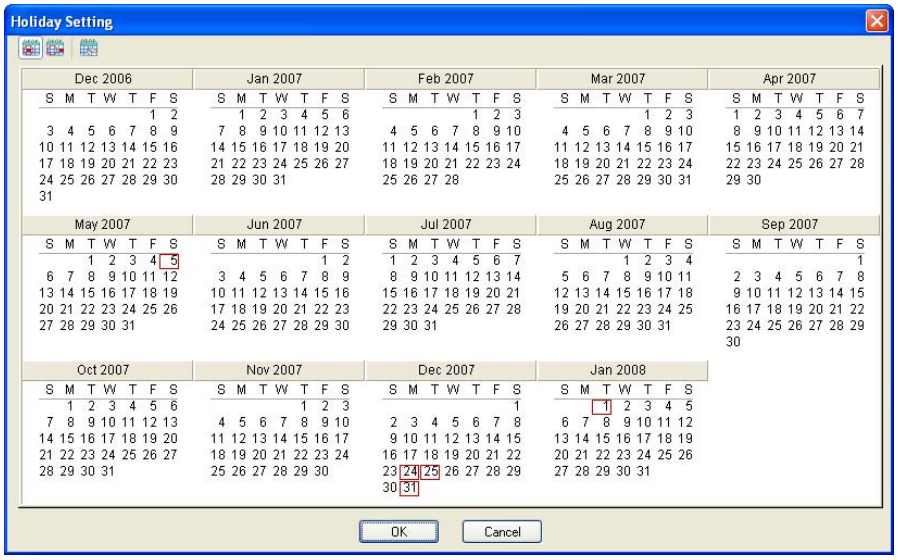


Figure 4-16

2. Cliquez sur l'icône **Jours fériés** et cliquez sur les dates des jours fériés. Par exemple,
   - Déc. 24, 2007 – Veille de noël
   - Déc. 25, 2007 – Noël
   - Déc. 31, 2007 – Veille du nouvel an
   - Jan 01, 2008 – Nouvel an
3. Pour effacer un jour férié, cliquez sur l'icône **Jour non férié** et cliquez sur la date que vous voulez effacer.

Remarque : Les dates des jours fériés peuvent dépasser le Nouvel an et certaines dates peuvent changer d'une année à l'autre. Les administrateurs doivent donc vérifier et mettre à jour les dates des jours fériés avant le début d'une nouvelle année pour garantir que les vacances sont correctement définies.

4.5 Réglage des Groupes d’accès

Les Groupes d’accès permettent de contrôler qui peur avoir accès à telle heure et à telle porte. Pour avoir accès à une porte sécurisée, un utilisateur doit passer les critères du groupe d’accès. L'utilisateur doit être à une porte qui accepte les membres de ce groupe d’accès et il doit être présent à une heure où l’accès est permis par un planning hebdomadaire.

Cette section utilise un exemple pour expliquer comment faire pour créer un groupe d’accès et assigner les critères du groupe d’accès à un badge. Dans cet exemple, le personnel FAE du poste de jour a besoin d’avoir accès aux portes de devant et de derrière pendant les heures du poste de jour.

1. Dans la barre de menu, cliquez sur **Configuration** et choisissez **Groupes d’accès**. La boîte de dialogue suivante s’affiche.

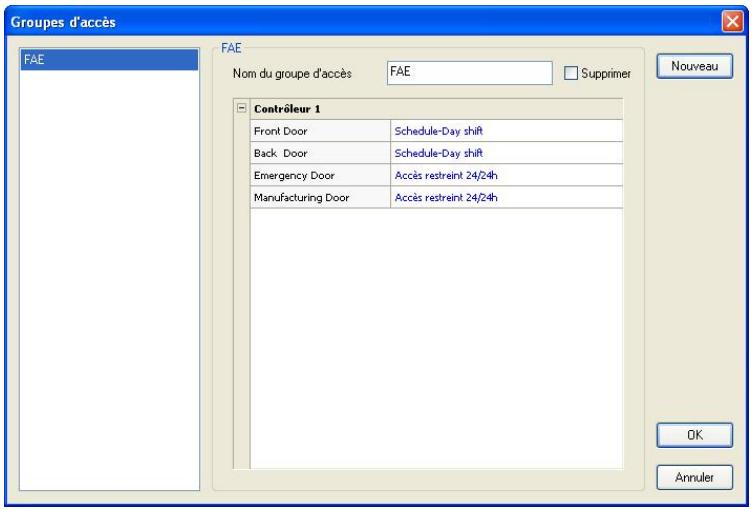


Figure 4-17

2. Cliquez sur le bouton **Nouveau** et entrez le **Nom** du nouveau groupe d’accès. Par exemple, nommez le groupe d’accès **FAE**.
3. Pour définir l’accès des portes pour le groupe d’accès, cliquez sur la liste déroulante de chaque porte et choisissez l’un des Plannings hebdomadaires prédéfinis. Par exemple, cliquez sur chaque champ bleu de **Porte de devant (Front Door)** et **Porte de derrière (Back Door)** puis choisissez **Planning – Poste de jour (Schedule-Day shift)**.
4. Cliquez sur **OK**. Le groupe d’accès pour le personnel FAE a été créé.
5. Pour assigner les critères du groupe d’accès sur un seul badge, cliquez sur **Personnel** dans la barre de menu et choisissez **Badges**. La boîte de dialogue Liste de badges s’affiche.
6. Double-cliquez sur un badge dans la liste. La boîte de dialogue suivante s’affiche.

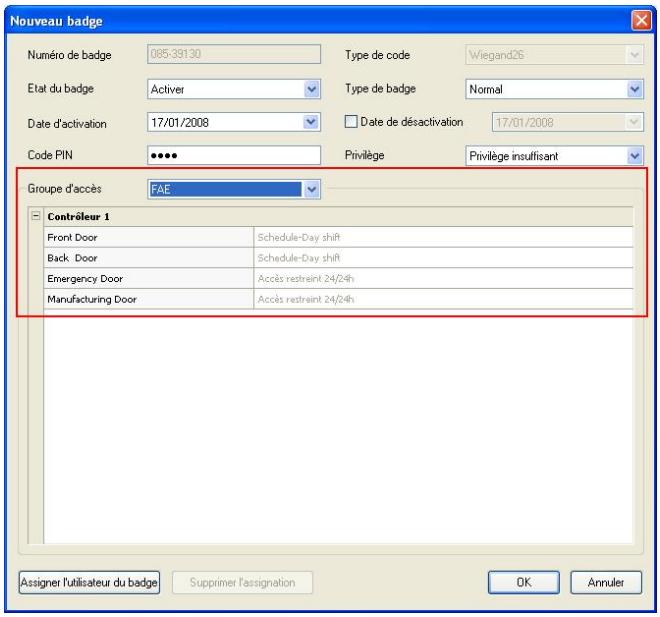


Figure 4-18

7. Dans la liste déroulante **Groupe d'accès**, choisissez un groupe d'accès prédéfini, par ex. **FAE**. Le Planning hebdomadaire correspondant s'affichera dans le champ de la porte correspondante.

4.6 Réglage des Utilisateurs de badge

Cette section décrit comment faire pour créer une base de données des informations d'utilisateurs de badge et comment faire pour assigner des badges à des utilisateurs.

4.6.1 Ajouter un Utilisateur de carte

1. Dans la barre de menu, cliquez sur **Personnel** et choisissez **Utilisateurs**. La fenêtre Liste d'utilisateurs s'affiche.
2. Cliquez sur le bouton **Nouveau** dans la barre d'outils. La boîte de dialogue suivante s'affiche.

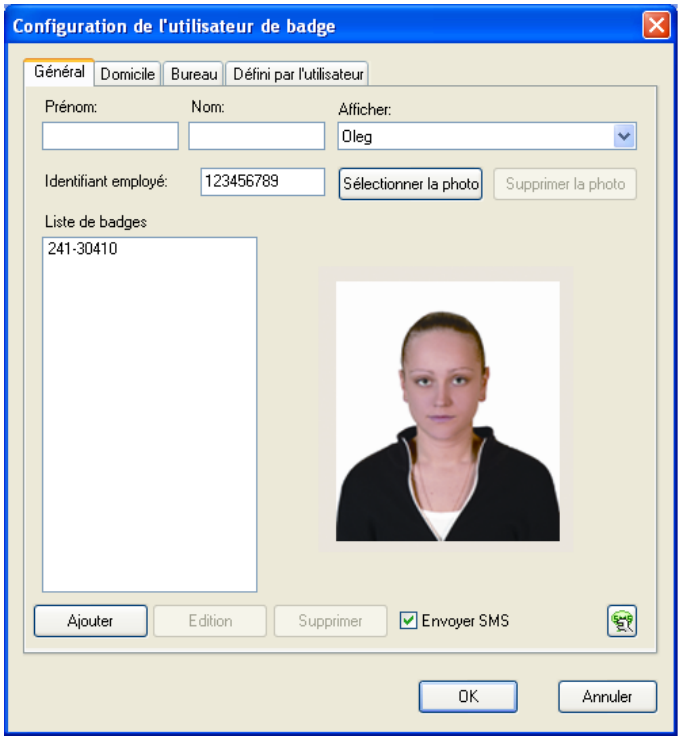


Figure 4-19

3. Entrez au moins un nom dans **Affichage** pour l'enregistrement. Les autres informations de l'utilisateur de badge, comme Identifiant employé, Photo, Domicile et Société sont optionnelles.

4.6.2 Assigner un Badge à un Utilisateur

Il y a deux méthodes pour assigner un badge à un utilisateur :

Remarque : Dans cette étape, nous supposons que vous avez suivi les instructions de la section *4.3 Réglage des Badges* pour terminer la création d'un badge.

---

1. Dans la boîte de dialogue Configuration de l'utilisateur de badge ci-dessus, cliquez sur **Ajouter** pour assigner le/les badge(s) à l'utilisateur.
2. Dans la boîte de dialogue Nouveau badge (voir Figure 4-18), sélectionnez **Assigner l'utilisateur du badge** et double-cliquez sur un utilisateur de badge dans la liste pour assigner l'utilisateur au badge.

4.6.3 Envoyer des alertes SMS

Si vous voulez envoyer des alertes SMS lorsque le(s) badge(s) assigné(s) à un utilisateur est utilisé dans le lecteur, sélectionnez **Envoyer SMS** dans la boîte de dialogue Configuration Utilisateur de badge.

Avant d'envoyer le SMS, voir la section *7.2.1 Configuration du Serveur SMS* pour configurer le serveur SMS. Pour plus d'informations sur les réglages des alertes SMS, voir les mêmes réglages de « Envoyer des alertes SMS » dans l'étape 3 de la section 7.2.3 de *Configuration des Notifications*.

4.6.4 Personnaliser un champ de données

Vous pouvez personnaliser les champs de données des utilisateurs de badge. Vous pouvez créer jusqu'à dix champs de données pour entrer les données des utilisateurs.

Lorsqu'un champ de données est créé, la description du champ sera affichée dans l'onglet Défini par l'utilisateur dans la boîte de dialogue Configuration de l'utilisateur de badge. Les données personnelles de chaque utilisateur sont entrées dans l'onglet Défini par l'utilisateur.

Pour personnaliser un champ de données :

1. Dans la barre de menu, cliquez sur **Personnel** et choisissez **Utilisateurs**. La fenêtre Liste d'utilisateurs s'affiche.
2. Cliquez sur le bouton **Configuration des champs par utlisateur** dans la barre d'outils. La boîte de dialogue Configuration des champs par utlisateur apparaît.
3. Sélectionnez un champ **Défini par l'utilisateur**, et entrez le texte que vous voulez afficher dans le champ de description. Dans cet exemple, le champ Car License Plate (Plaque immatriculation de véhicule) a été créé.

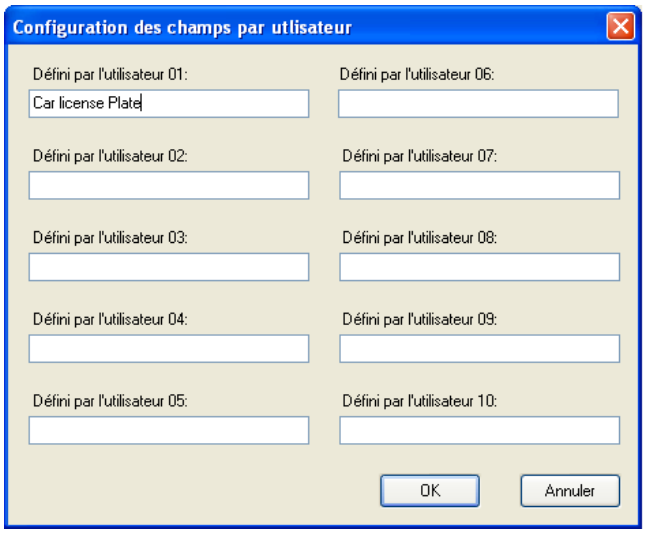


Figure 4-20

Pour entrer des données personnelles :

1. Dans la barre de menu, cliquez sur **Personnel** et choisissez **Utilisateurs**. La fenêtre Liste d'utilisateurs s'affiche.
2. Double-cliquez sur l'utilisateur dans la liste pour lequel vous voulez entrer des données personnelles. La boîte de dialogue **Configuration des champs par utlisateur** s'affiche.
3. Cliquez sur l'onglet **Défini par l'utilisateur**. Le champ de données personnalisé que vous avez créé est maintenant visible.
4. Cliquez sur le champ de données personnalisées et entrez les informations requises. Dans cet exemple, un numéro a été entré dans le champ **Car License Plate (Plaque immatriculation de véhicule)** :

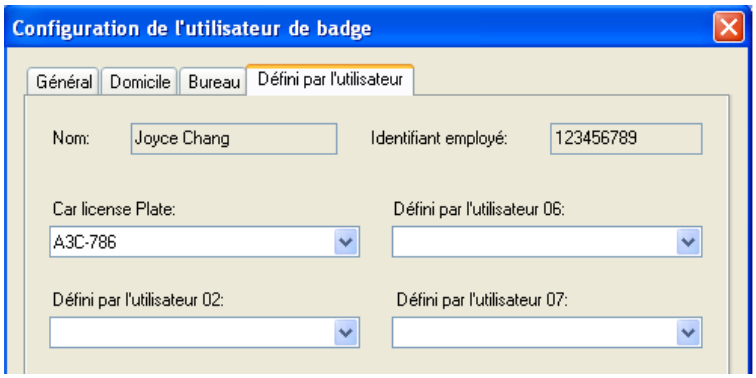


Figure 4-21

4.6.5 Importer/Exporter les données des utilisateurs de badge

Dans la fenêtre Liste d'utilisateurs, vous pouvez importer et exporter les données des utilisateurs de badges aux formats mdb et xls. Pour plus d'informations sur cette fonction, voir *4.3.3 Importer/Exporter les données des badges.*

Chapitre 5 Intégration vidéo

Les produits IP de GeoVision et certaines caméras IP de tiers peuvent être connectés à ASManager via le réseau. La vidéo en direct peut alors être accédée pour la surveillance et le contrôle.

ASManager offre les fonctions vidéo suivantes :

- Vue en direct
- Lecture vidéo
- Contrôle jusqu'à 16 caméras à la fois

Remarque :

- Les produits IP GeoVision comprennent GV-System, GV-NVR, GV-Vidéo serveur, GV-Compact DVR et GV-IP caméra. Pour les caméras IP de tiers, voir Appendice.
- ASManager ne supporte que GV-System avec la version 8.120 ou plus récent.

Conseil : Dans les sections suivantes, le terme « DVR » indique GV-System et GV-NVR, le terme « Serveur vidéo » indique le serveur GV-Video Server et le terme « DVR Compact » indique GV-Compact DVR.

5.1 Mapping de caméras

Si vous voulez mapper une caméra d'un DVR à une porte, le DVR doit être activé pour l'accès vidéo :

- Activer le **Serveur de centre de contrôle** (CCS)

Pour affecter une caméra à une porte :

1. Dans la barre de menu, cliquez sur **Configuration** et choisissez **Périphérique**. La boîte de dialogue Liste des contrôleurs s'affiche.
2. Double-cliquez sur un contrôleur dans la liste. La boîte de dialogue Configuration contrôleur s'affiche.

3. Cliquez sur un onglet **Porte**. La boîte de dialogue suivante s'affiche.

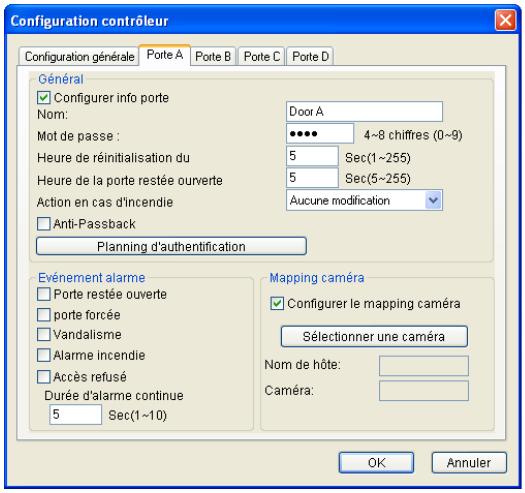


Figure 5-1

4. Dans la section Mapping caméra, sélectionnez **Configurer le mapping caméra** et cliquez sur **Sélectionner une caméra**. La boîte de dialogue suivante s'affiche.

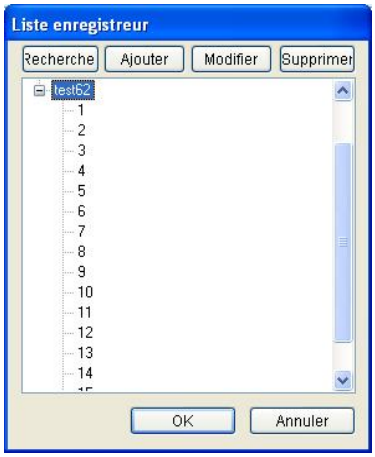


Figure 5-2

5. Pour connecter une périphérique à ASManager, utilisez l'une des méthodes suivantes :
   - Cliquez sur **Ajouter**, sélectionnez le type d'appareil IP et entrez son adresse IP unique.
   - Cliquez sur **Recherche** pour détecter tous les appareils IP de GeoVision sur le même LAN

   Dans les étapes suivantes, nous utilisons la première méthode pour établir une connexion avec l'enregistreur comme exemple.
6. Cliquez sur **Ajouter** et sélectionnez **Ajouter mapping DVR** pour mapper une caméra d'un DVR à la porte.
7. Dans la boîte de dialogue Configuration d'hôte, entrez le **Nom d'hôte**, l'**Adresse IP**, l'**Identifiant** et le **Mot de passe** de l'enregistreur.
8. Cliquez sur **OK**. L'enregistreur sera affiché dans boîte de dialogue Liste enregistreur.

9. Ouvrez le dossier Enregistreur, choisissez une caméra et cliquez sur **OK**. Le **Nom d'hôte** et la **Caméra** seront affichés dans la boîte de dialogue Configuration contrôleur.
10. Cliquez sur **OK** pour retourner à l'écran principal.
11. Cliquez sur la porte spécifiée dans la fenêtre Device View (Visualisation périphérique). La vue en direct correspondante apparaît.

Remarque : Si vous utilisez la fonction **Recherche** pour ajouter des appareils IP de GeoVision. Vous devez alors cliquer sur le bouton **Modifier** pour entrer les identifiants et les mots de passe ; autrement aucune vue en direct ne s'affichera.

5.2 Accéder à une Vue en direct

Après avoir mappé les caméras aux portes, utilisez l'une des méthodes suivantes pour accéder à la vue en direct dans la fenêtre Vue en direct (voir Figure 3-1) :

- Dans la fenêtre Visualisation périphérique, cliquez sur la porte désirée. La vue en direct correspondante apparaît.
- Dans la fenêtre Liste caméras, cliquez sur la caméra désirée. La vue en direct correspondante apparaît.
- Dans les fenêtres Fenêtre d'alarme et Fenêtre d'accès, cliquez sur l'événement désiré. La vue en direct correspondante apparaît.

Pour accéder à une vue en direct de plusieurs appareils IP, voir *5.4 La fenêtre Multi-vue* ci-dessous.

5.3 Accéder à une image vidéo

Vous pouvez accéder à l'image vidéo des accès et des événements d'alarme.

- Dans la Fenêtre d'accès et la Fenêtre d'alarme, double-cliquez sur l'événement désiré pour afficher l'image. Ou cliquez avec le bouton droit sur l'événement désiré et choisissez **Afficher l'image** pour afficher l'image. Si aucune image n'est disponible, l'option sera en gris.

5.4 La fenêtre Multi-vue

La fenêtre Multi-vue offre une vue rapide de jusqu'à 16 caméras prédéfinis sur un seul écran. Ces caméras peuvent être une combinaison d'un ou de plusieurs appareils IP.

Pour ouvrir et utiliser la fenêtre Multi-vue :

1. Dans la barre de menu, cliquez sur **Visualisation** et choisissez **Multi-vue**. La fenêtre Multi-vue apparaît, similaire à Figure 5-3.
2. Faites glisser la caméra désirée de la fenêtre Visualisation périphérique ou Liste caméras vers le cadre désiré dans la fenêtre Multi-vue.

La vidéo de la caméra apparaît dans ce cadre. Si la vue d'une autre caméra existe déjà dans ce cadre, la nouvelle vidéo la remplacera.

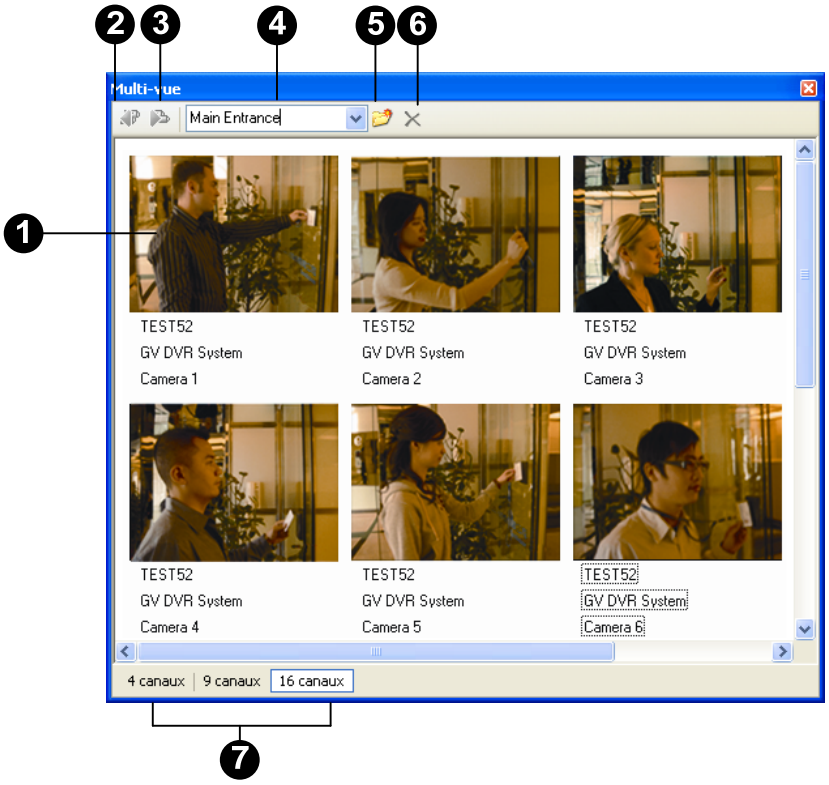


Figure 5-3

Les contrôles de la fenêtre Multi-vue sont décrits ci-dessous :

Nº	Nom	Fonction
1	Cadre	Affiche la vidéo en direct de la caméra que vous avez glissée et déposée.
2	Page précédente	Pour retourner à la page précédente des vues de caméra.
3	Page suivante	Pour aller à la page suivante des vues de caméra.
4	Vue Matrice	Sélectionnez une Vue Matrice existante (un groupe de vues) dans la liste déroulante. Pour plus de détails, voir *5.4.1 Ajouter une Vue Matrice*.
5	Ajouter Matrice	Pour ajouter une Vue Matrice.
6	Supprimer Matrice	Pour supprimer une Vue Matrice.
7	Affichage canaux	Pour afficher 4, 9 ou 16 canaux sur l'écran.

Remarque : Il est possible de glisser la fenêtre Multi-vue hors de l'écran principal et même de glisser la fenêtre pour la placer sur le moniteur d'un deuxième ordinateur.

5.4.1 Ajouter une Vue Matrice

Une Vue Matrice, ou un groupe de vues, est un arrangement préprogrammé des cadres dans la fenêtre Multi-vue qui permet d'afficher jusqu'à seize vues de caméra différentes. Une Vue Matrice peut être ajoutée comme désiré.

1. Dans la liste déroulante Vue Matrice, entrez un nom pour la Vue Matrice.
2. Cliquez sur le bouton **Ajouter Matrice**. Le nom de la Vue Matrice est créé dans la liste déroulante Vue Matrice.
3. Faites glisser la caméra désirée de la fenêtre Visualisation périphérique ou Liste caméras vers le cadre désiré dans la fenêtre. La vidéo de la caméra apparaît dans ce cadre.
4. Vous pouvez répéter les Etapes 1-3 pour ajouter plus d'une Vue Matrice. Et utilisez la liste déroulante pour changer à une Vue Matrice différente.

5.5 Récupérer des vidéos enregistrées

Les vidéos enregistrées peuvent être regardées en récupérant ces vidéos des produits IP de GeoVision et en les jouant. Avant de pouvoir regarder une vidéo enregistrée sur la périphérique IP de GeoVision, la fonction suivante doit être activée pour permettre l'accès à distance :

- Enregistreur : Cochez l'option **Service de ViewLog à distance** dans le Serveur de centre de contrôle
- Serveur vidéo, Enregistreur compact : Cochez l'option de la fonction **ViewLog à distance**

Remarque : La caméra GV-IP ne supporte pas la fonction de lecture.

Pour regarder une vidéo :

- Dans la Fenêtre d'accès et la Fenêtre d'alarme, cliquez sur l'événement désiré. Si la vidéo enregistrée existe, la fenêtre Lecture sera activée. Cliquez sur le bouton **Lecture** pour commencer la lecture du clip vidéo.

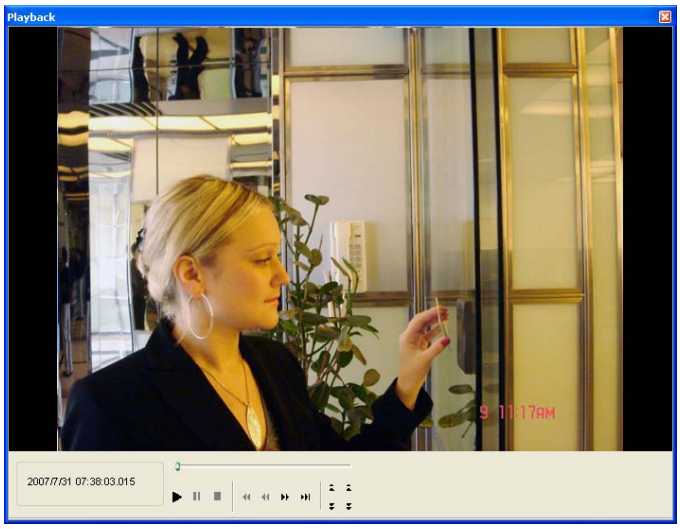
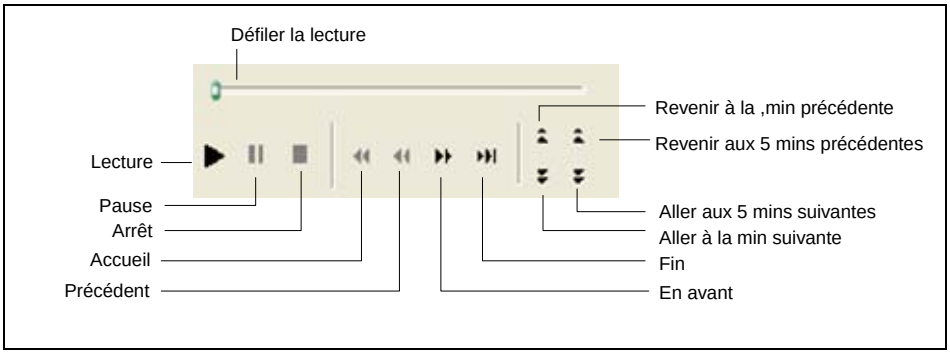


Figure 5-4



Cliquez avec le bouton droit sur la fenêtre pour afficher les fonctions suivantes :

Mode de lecture	Contient les options suivantes : • **Image par image :** Pour avancer image par image dans la lecture. • **Temps réel :** Pour lire la vidéo en temps réel. Ce mode économise le temps de rendu, mais des images ne sont pas affichées pour donner l'apparence d'une lecture en temps réel. • **Lecture automatique de 5 minutes suivantes :** Pour lire jusqu'à 5 minutes de vidéo. • **Audio :** Pour couper/remettre le son du clip vidéo.
Appliquer le rendu	Contient les options suivantes : • **Désentrelacement :** Pour convertir la vidéo entrelacée en une vidéo non-entrelacée. • **Dépixelisation :** Pour adoucir les carrés de mosaïque lorsque vous agrandissez une lecture vidéo. • **Déblocking :** Pour supprimer les artefacts de bloc des clips vidéo de basse qualité et hautement compressée. • **Réduction du brouillard :** Améliore la visibilité de l'image. • **Stabilisation :** Réduit les tremblements de la caméra. • **Affichage texte du nom de la caméra et de l'heure :** Pour afficher le nom de la caméra et l'heure sur la vidéo. • **Affichage texte POS/GV-Wiegand :** Pour afficher les données POS ou Capture GV-Wiegand sur la vidéo. • **Plein écran :** Pour aller au mode d'affichage plein écran.
Outils	• **Cliché :** Pour enregistrer la prise la photo de la vidéo. • **Enregistrer sous AVI :** Pour enregistrer la vidéo au format AVI. • **Télécharger :** Pour télécharger la vidéo des produits IP de GeoVision sur l'ordinateur local.

Chapitre 6 ASLog

Le ASLog affiche les informations des événements des portes du jour. Les journaux sont affichés avec un message d'accès, le nom de l'utilisateur du badge, le nom de la porte et l'heure locale. Vous pouvez aussi accéder aux images et afficher les séquences vidéos si disponibles.

Pour afficher ASLog :

1. Pour afficher ASlog, cliquez sur **Outils** dans la barre de menu et choisissez **ASLog**. La fenêtre suivante s'affiche.

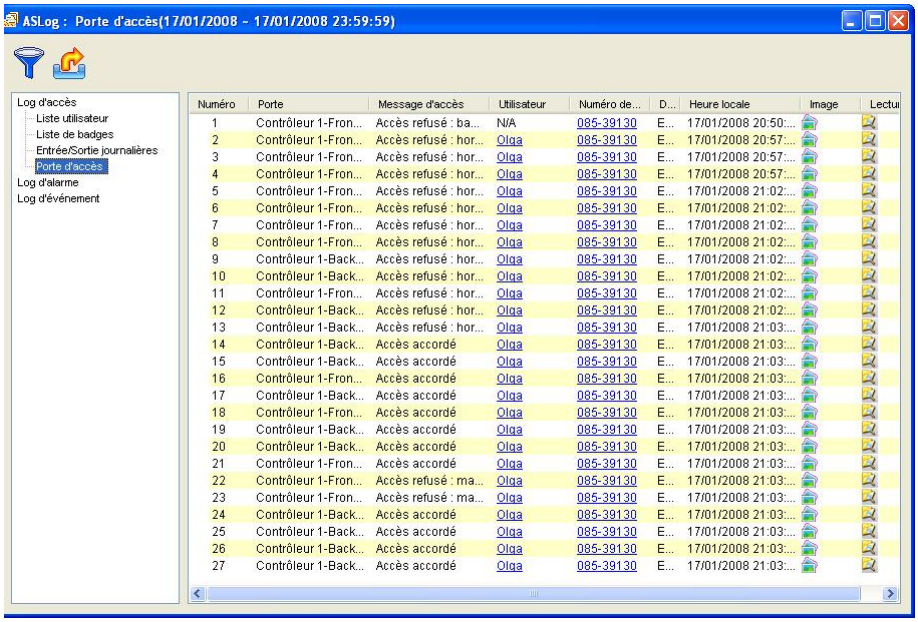


Figure 6-1

2. Dans le coté gauche, choisissez le critère de triage, par exemple Porte d'accès. Les événements du jour seront affichés en fonction de votre sélection.
3. Pour afficher les journaux des jours précédents, cliquez sur le bouton **Filtre**. Choisissez ensuite le critère de recherche pour trouver les événements désirés.
4. Pour exporter les résultats de la recherche, cliquez sur le bouton **Exporter**. Enregistrez les résultats sous un fichier **.txt**, **.xls** ou **.htm**.

Remarque : Vous pouvez relire la vidéo seulement lorsque le Service ViewLog à distance dans le Serveur du centre de contrôle est activé sur l'enregistreur. Et la fonction ViewLog à distance est activée sur le Serveur vidéo ou sur le compact DVR.

Chapitre 7 Autres fonctions

7.1 Réglage d'un utilisateur du système

Un utilisateur du système est une personne qui utilise ASManager pour vérifier les contrôleurs de porte, pour enregistrer des utilisateurs de badge ou pour programmer le système. L'administrateur du système peut, grâce à cette fonction, créer des nouveaux utilisateurs du système avec des droits d'accès différents. Il est possible de créer jusqu'à 1 000 comptes d'utilisateurs.

7.1.1 Ajouter un nouvel utilisateur

1. Dans la barre de menu, cliquez sur **Outils** et choisissez **Comptes**. La boîte de dialogue suivante s'affiche.

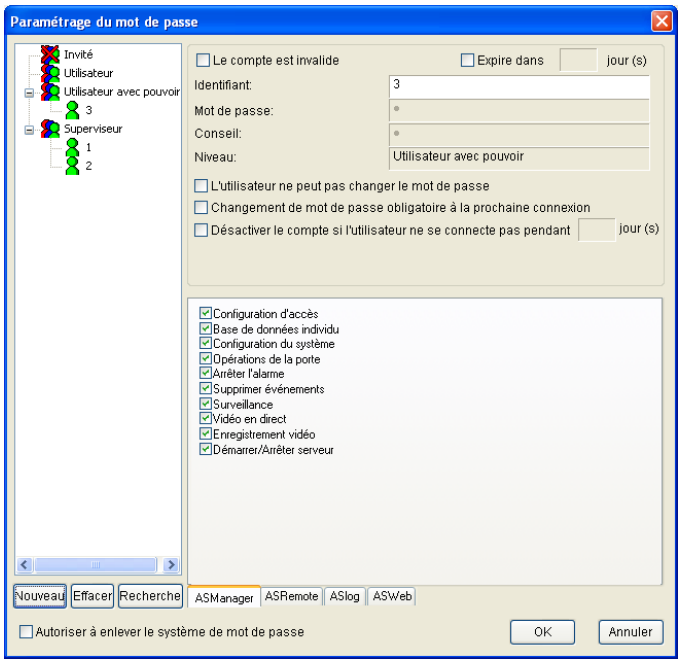


Figure 7-1

2. Cliquez sur **Nouveau** en bas à gauche. La boîte de dialogue suivante s'affiche.

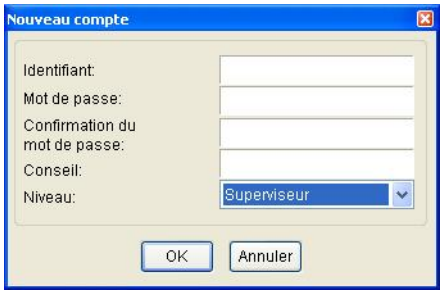


Figure 7-2

3. Entrez l'**Identifiant** et le **Mot de passe** de l'utilisateur. Entrez de nouveau le mot de passe dans le champ Confirmation du mot de passe.
4. Entrez aussi un **Conseil** (en option) pour vous aider si vous oubliez le mot de passe.
5. Choisissez le niveau d'autorisation de l'utilisateur : **Superviseur**, **Utilisateur avec pouvoir** ou **Utilisateur**. Par défaut, les utilisateurs avec le niveau Superviseur possèdent tous les droits et tous les privilèges de réglage du système. Les Utilisateurs avec pouvoir ont les mêmes droits et privilèges que les Superviseurs, sauf qu'ils ne peuvent pas éditer les informations des utilisateurs et supprimer le mot de passe du système (décrit ci-dessous). Les utilisateurs de base ne peuvent pas accéder aux réglages du système et n'a qu'un accès limité à certaines fonctions.
6. Cliquez sur **OK** pour ajouter l'utilisateur.
7. Cliquez sur l'onglet **ASManager**, **ASRemote**, **ASLog** ou **ASWeb**

. Cochez et décochez les fonctions que l'utilisateur du système peut avoir accès.
8. Autres réglages disponibles :
   - **Expire dans xx jour(s) :** Le compte expirera et sera automatiquement désactivé après un certain nombre de jours. Le nombre que vous entrez ici sera automatiquement utilisé. Entrez un nombre compris entre 1 et 9999.
   - **L'utilisateur ne peut pas changer le mot de passe :** L'utilisateur n'a pas le droit de changer le mot de passe.
   - **Changement de mot de passe obligatoire à la prochaine connexion :** L'utilisateur devra changer le mot de passe lorsqu'il se connecte la première fois.
   - **Désactiver le compte si l'utilisateur ne se connecte pas pendant xx jour(s) :** Si l'utilisateur ne se connecte pas au système pendant un certain nombre de jours, son compte sera automatiquement désactivé.
   - **Autoriser à enlever le système de mot de passe :** Cette option permet à l'utilisateur d'effacer l'identifiant et le mot de passe de la base de données du système. Pour faire cela, cochez cette option (seulement un Superviseur peut cocher cette option) et trouvez **PassUnInStall** dans le dossier système. Cliquez sur le programme ; un message s'affiche, vous invitant à confirmer. Cliquez sur **Oui** pour effacer l'Identifiant et le mot de passe du système.

Remarque : Si l'option **Autoriser à enlever le système de mot de passe** n'est pas cochée, la perte des mots de passe forcera la réinstallation de Windows et la réinitialisation des mots de passe.

7.1.2 Editer un utilisateur existant

Seulement les superviseurs peuvent éditer les informations d'un utilisateur du système.

1. Choisissez un utilisateur dans la liste des utilisateurs pour afficher ses propriétés. Ou cliquez avec le bouton droit sur l'un des niveaux d'utilisateur (Utilisateur, Utilisateur avec pouvoir, Superviseur) puis choisissez **Trouver un compte spécifique** pour une recherche rapide. Un mot de passe valide doit être entré pour éditer les informations d'un superviseur.
2. Editez les propriétés comme désiré. Cochez l'option **Compte est désactivé** si vous voulez désactiver cet utilisateur.

7.1.3 Modifier le mot de passe lors de la connexion

1. Lorsque vous vous connectez au système, cliquez sur **Modifier le mot de passe** dans la boîte de dialogue Connecter. La boîte de dialogue Modifier le mot de passe s'affiche.

Figure 7-3

2. Entrez le nouveau mot de passe et cliquez sur **OK** pour enregistrer les modifications.

Remarque : Si l'utilisateur n'a pas le droit de changer le mot de passe, le message *Erreur modifier le mot de passe/Conseil* s'affichera.

7.2 Configuration de notification

Lorsque des conditions d'alarme se présentent, le système peut automatiquement activer l'alarme de l'ordinateur et envoyer des alertes par SMS et par email à une ou plusieurs personnes.

7.2.1 Configuration du serveur SMS

Avant de pouvoir envoyer des alertes par SMS, vous devez configurer le serveur SMS.

1. Dans la barre de menu, cliquez sur **Outils** et choisissez **Configuration du serveur SMS**. La boîte de dialogue suivante s'affiche.

Figure 7-4

2. Entrez l'adresse IP du serveur SMS, le nom d'utilisateur et le mot de passe pour la connexion. Puis choisissez jusqu'à trois numéros de téléphone portable, avec l'indicatif du pays, où les alertes par SMS doivent être envoyées. Cliquez sur **OK**.
3. Pour activer la connexion SMS, cliquez sur **Outils** dans la barre de menu et choisissez **Se connecter au serveur SMS**.

Remarque : Pour l'encodage ASCII (langue anglaise), les messages texte SMS sont limités à 160 caractères ; pour l'encodage Unicode (autres langues), les messages texte SMS sont limités à 70 caractères. Si vous voulez envoyer des messages texte plus long, sélectionnez **Envoyer plus d'un sms si le contenu est trop long**. Les longs messages seront divisés en un maximum de 9 parties et envoyés comme multiples messages SMS.

7.2.2 Configuration du serveur email

Avant de pouvoir envoyer des alertes par email, vous devez configurer le serveur email.

1. Dans la barre de menu, cliquez sur **Outils** et choisissez **Configuration du serveur email**. La boîte de dialogue suivante s'affiche.

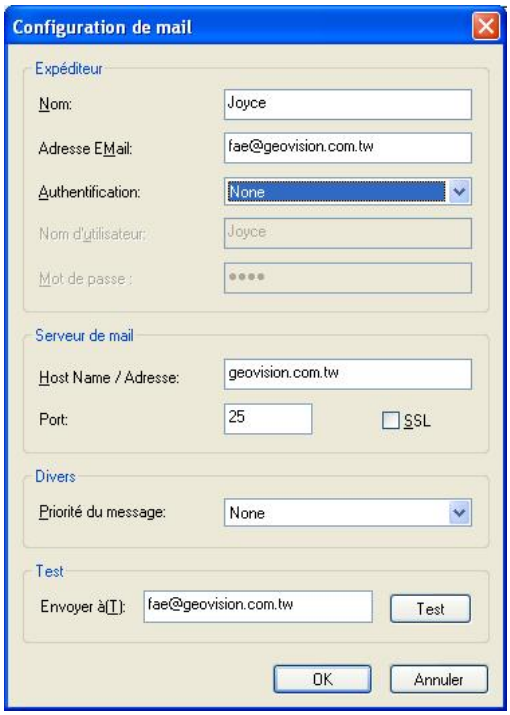


Figure 7-5

2. Réglez les options suivantes :
   - **Nom :** Entrez le nom de l'envoyeur.
   - **Adresse EMail :** Entrez l'adresse email de l'envoyeur.
   - **Authentification :** Si le serveur email a besoin d'une authentification pour envoyer les emails, choisissez une méthode d'authentification et entrez le nom d'utilisateur et le mot de passe.
   - **Nom d'hôte / Adresse :** Entrez le nom du serveur email.
   - **Port de commande :** Laissez le réglage sur le port par défaut 25 ou changez-le sur le même que le serveur email.
   - **SSL :** Activez le protocole SSL (Secure Sockets Layer) pour augmenter la sécurité et l'anonymat de la connexion Internet. Lorsque cette option est cochée, le Port change sur 465.
   - **Priorité du message :** Choisissez le niveau de priorité pour que le destinataire sache s'il doit le lire immédiatement (haute priorité) ou s'il peut le lire plus tard lorsqu'il a le temps (priorité basse). Un message de haute priorité a un point d'exclamation à côté du message. Un message de basse priorité est indiqué par une flèche vers le bas.

- **Envoyer à :** Entrez une adresse email valide et cliquez sur le bouton **Test** pour vérifier si la configuration du serveur est correctement faite.

7.2.3 Configuration des notifications

1. Dans la barre de menu, cliquez sur **Outils** et choisissez **Notifications**. La boîte de dialogue suivante s'affiche.

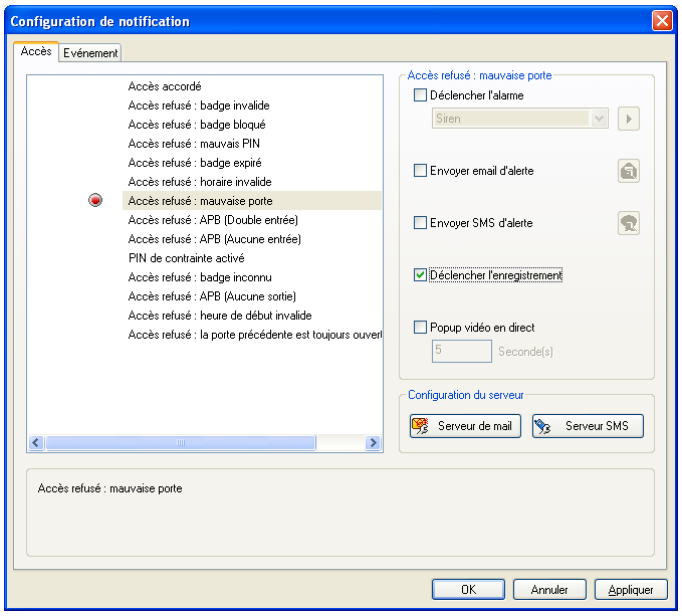


Figure 7-6

2. Utilisez les onglets **Accès** et **Evénement** pour choisir un événement désiré pour la configuration de l'alerte.
3. Définissez les méthodes d'alerte suivantes :
   - **Déclencher l'alarme :** Pour activer l'alarme de l'ordinateur lorsque l'événement sélectionné se produit.
   - **Envoyez email d'alerte :** Lorsque vous cochez cette option, un email s'affichera. Entrez l'adresse email du destinataire et le sujet de l'alerte. Puis entrez le contenu désiré ou utilisez les boutons de la fenêtre de texte pour envoyer automatiquement les informations programmées.
     Par exemple, si vous cliquez sur le bouton , l'alerte SMS envoyé contiendra les informations du contrôleur. Pour plus de détails, voir *Symboles d'alerte Email et SMS* dans Appendice.
   - **Envoyer SMS d'alerte :** Lorsque vous cochez cette option, une boîte de dialogue s'affichera. Assurez-vous que les numéros des téléphones portables ont été réglés. Sélectionnez **Type de code du texte**. Puis entrez vos messages ; vous pouvez aussi cliquer sur les boutons de la fenêtre de texte pour envoyer automatiquement

les informations programmées. Voir l'exemple ci-dessus dans « Envoyer Email d'alerte ».

- **Déclencher l'enregistrement :** Active l'enregistrement de l'enregistreur, du Serveur vidéo ou de l'enregistreur compact lorsque l'événement sélectionné se produit. La durée d'enregistrement est entre 3 et 6 secondes.
- **Popup vidéo en direct :** Une fenêtre de vue en direct s'affichera lorsque l'événement sélectionné se produit. Vous pouvez aussi spécifier la durée de l'affichage de la vue en direct sur l'écran, jusqu'à 300 secondes.

4. Pour définir plus d'un événement avec la même configuration d'alerte, cliquez en premier avec le bouton droit sur l'événement défini dans la liste et sélectionnez **Copier** pour enregistrer les réglages. Puis utilisez Ctrl + clic gauche ou Shift + clic gauche pour sélectionner plusieurs événements. Cliquez avec le bouton droit sur les événements sélectionnés et choisissez **Coller** pour utiliser les mêmes réglages.

Remarque : Pour le type de code de texte, choisissez **ASCII** pour le texte anglais, limité à 160 caractères, et choisissez **Unicode** pour le texte dans d'autres langues, limité à 70 caractères.

7.3 Configuration de démarrage et de sauvegarde

Vous pouvez sélectionner quel serveur doit être activé au démarrage de Windows ou de ASManager.
Vous pouvez aussi spécifier un chemin pour la fonction **Sauvegarde automatique** pour enregistrer automatiquement une copie des journaux et des fichiers images. Le journal et les fichiers images sont enregistrés par défaut dans :\ASManager\ASRes.

- Pour accéder à ces fonctions, cliquez sur **Outils** dans la barre de menu et choisissez **Option**.

Chapitre 8 ASRemote

Le logiciel client ASRemote a été conçu pour contrôler plusieurs ASManager sur le réseau. ASRemote offre les fonctions suivantes :

- Surveillance à distance
- Vue en direct et lecture à distance
- Contrôle à distance : Arrêter les alarmes et forcer l'ouverture/la fermeture des portes.

8.1 Installation de ASRemote

Insérez le CD du programme dans votre ordinateur ; une fenêtre s'affichera automatiquement. Choisissez **Install GeoVision V1.1 Access Control System (Installer le système de contrôle d'accès GeoVision V1.1)**, cliquez sur **GeoVision Access Control System (Système de contrôle d'accès GeoVision)** et suivez les instructions à l'écran pour terminer l'installation.

8.2 La fenêtre de ASRemote

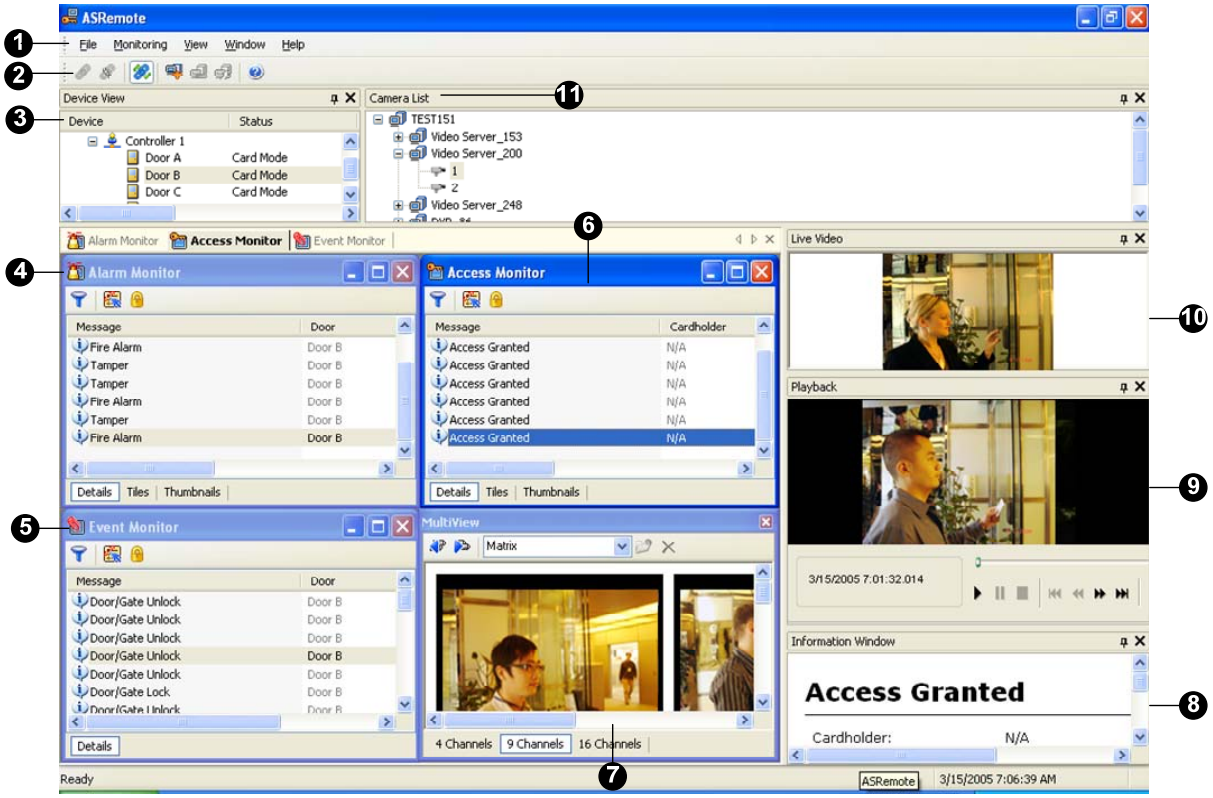


Figure 8-1

Nº	Nom	Fonction
1	Barre de menu	La Barre de menu permet d'accéder aux menus **Fichiers** (connexion/déconnexion de ASManager), **Enregistrement en cours** (afficher les fenêtres de surveillance des alarmes, des accès et des événements), **Affichage** (afficher les fenêtres de fonction) et **Fenêtre** (arranger l'affichage des différentes fenêtres).
2	Barre d'outils	La Barre d'outils contient les options **Connecter, Déconnecter, Connexion automatique, Ajouter l'hôte, Supprimer l'hôte, Configuration** et **A propos de ASRemote**.
3	Visualisation périphérique	Affiche une liste des portes connectées et leurs états.
4	Fenêtre d'alarme	Affiche les événements d'alarme des portes.
5	Fenêtre d'événement	Affiche les événements surveillés des portes.
6	Fenêtre d'accès	Affiche les activités d'accès des portes.

7	Multi-vue	Affiche les vues en direct des caméras connectées de multiples caméras IP. Pour plus de détails, voir « Fenêtre Multi-vue » dans Chapitre 5.
8	Fenêtre d'information	Affiche les informations des portes, des lecteurs de badge et des événements surveillés.
9	Lecture	Relit les événements enregistrés à partir d'un périphérique IP GeoVision compatible. Pour plus de détails, voir la même opération dans « Récupérer les vidéo enregistrées » dans Chapitre 5.
10	Vidéo en direct	Affiche les fenêtres de vue en direct d'une caméra connectée. Pour plus de détails, voir la même opération dans « Accéder à la vue en direct » dans Chapitre 5.
11	Liste des caméras	Affiche une liste de toutes les caméras connectées.

8.2.1 Barre d'outils

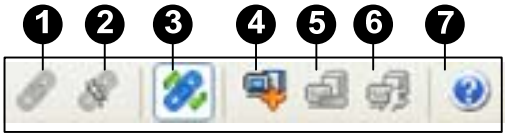


Figure 8-2

Les boutons de la Barre d'outils de ASRemote :

Nº	Nom	Fonction
1	Connecter	Démarre la connexion à ASManager.
2	Déconnecter	Termine la connexion à ASManager.
3	Connexion automatique	Essaye de se reconnecter à ASManager.
4	Ajouter l'hôte	Ajoute un hôte ASManager à la liste.
5	Supprimer l'hôte	Supprime un hôte ASManager de la liste.
6	Configuration	Configure les réglages des hôtes ASManager.
7	A propos de	Affiche la version de ASRemote.

8.3 Connexion à ASManager

Avant que ASRemote puisse se connecter à un ASManager, le ASManager doit être configuré pour permettre l'accès de la manière suivante :

- Dans la barre de menu, cliquez sur **Outils** puis choisissez **Serveurs** puis activez **Serveur de surveillance à distance**. Lorsque le serveur démarre, l'icône apparaît en bas de l'écran principal.

Pour créer un hôte ASManager et activer la connexion à ASManager :

1. Dans la barre d'outils, cliquez sur le bouton **Ajouter l'hôte**. La boîte de dialogue suivante s'affiche.

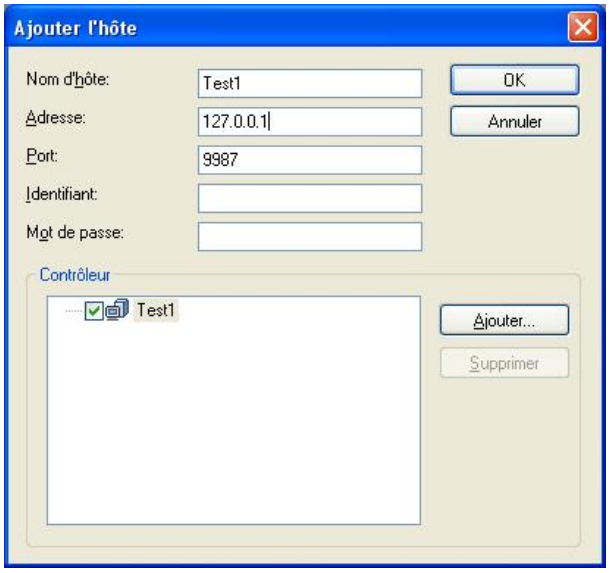


Figure 8-3

2. Entrez le nom d'hôte, entrez l'adresse IP du ASManager, changez le numéro du port si nécessaire et entrez l'identifiant et le mot de passe du ASManager.
3. Cliquez sur **Ajouter**. La boîte de dialogue suivante s'affiche.

Figure 8-4

4. Entrez l'identifiant du contrôleur associé au ASManager et cliquez sur **OK**.
5. Pour ajouter d'autres contrôleurs, répétez les Etapes 3-4.

6. Cliquez sur **OK** pour retourner à l'écran principal. Une liste de dossiers d'hôte s'affichera dans la fenêtre Visualisation périphérique comme indiqué ci-dessous.

Figure 8-5

Si l'icône est affichée, cela indique que la connexion entre ASManager et ASRemote a été établie.

Si l'icône est affichée, cela indique que la connexion a échoué. Vérifiez que l'ASManager est activé pour la fonction Serveur de surveillance à distance.

Chapitre 9 ASWeb

ASWeb a été conçu pour obtenir les données des événements à partir du ASManager sur le réseau. Avec une seule connexion à ASManager à la fois, les utilisateurs peuvent regarder les données des événements et aussi télécharger les journaux dans différents formats.

9.1 Connexion à ASManager

Avant que ASWeb puisse se connecter à un ASManager, le ASManager doit être configuré pour permettre l'accès de la manière suivante :

- Dans la barre de menu, cliquez sur **Outils** et choisissez **Serveurs** puis activez **WebServer**. La boîte de dialogue suivante s'affiche.

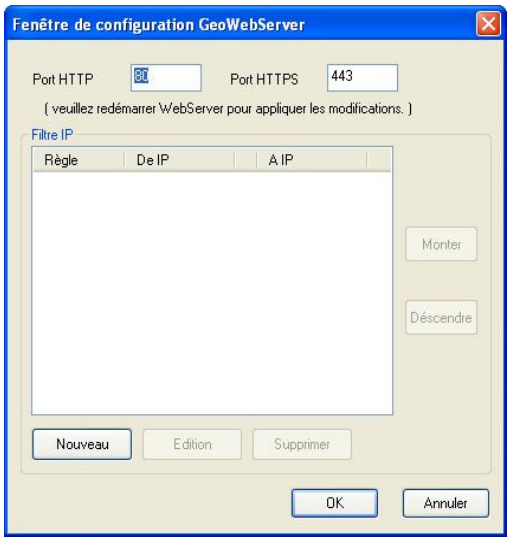


Figure 9-1

Si vous voulez permettre ou refuser l'accès à partir de certaines adresses IP, cliquez sur **Nouveau** et entrez les adresses IP. Autrement cliquez sur **OK** pour démarrer la connexion. Lorsque le serveur démarre, l'icône apparaît en bas de l'écran principal.

Pour démarrer ASWeb :

1. Ouvrez un navigateur Internet et entrez l'adresse IP du ASManager auquel vous voulez vous connecter.

   La page Web suivante s'affiche.

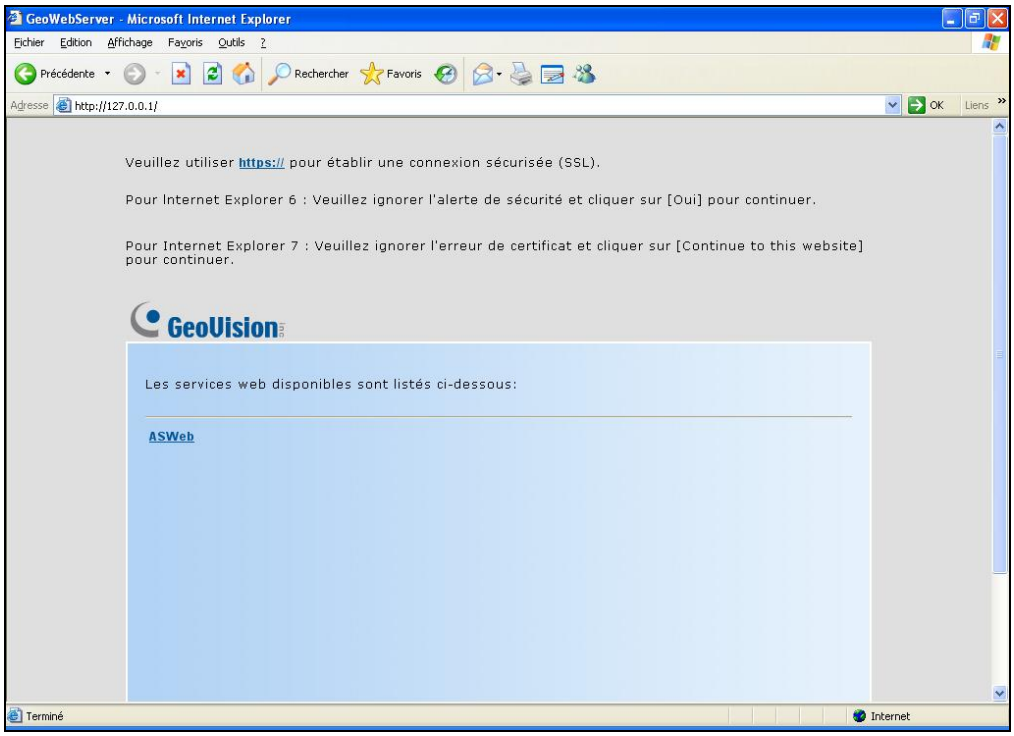

GeoWebServer - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente
Rechercher
Favoris
Adresse
http://127.0.0.1/
OK
Liens
Veuillez utiliser https:// pour établir une connexion sécurisée (SSL).
Pour Internet Explorer 6 : Veuillez ignorer l'alerte de sécurité et cliquer sur [Oui] pour continuer.
Pour Internet Explorer 7 : Veuillez ignorer l'erreur de certificat et cliquer sur [Continue to this website] pour continuer.
GeoVision
Les services web disponibles sont listés ci-dessous:
ASWeb
Terminé
Internet

Figure 9-2

2. Cliquez sur **https://** pour une connexion cryptée **SSL** ou sur l'**ASWeb** pour une connexion normale. Une boîte de dialogue de connexion s'affiche.

Figure 9-3

3. Entrez le nom d'utilisateur et le mot de passe du ASManager auquel vous voulez vous connecter. La page de l'ASWeb s'affiche.

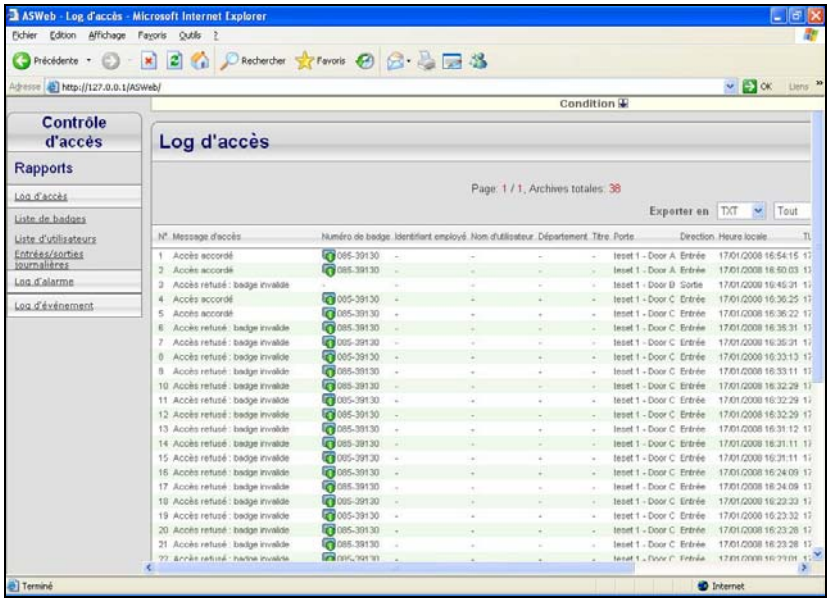


Figure 9-4

9.2 Accéder aux journaux

Vous pouvez accéder aux journaux du ASManager connecté, y-compris le Log d'accès, la Liste de badges, la Liste d'utilisateurs, les Entrées/sorties journalières, le Log d'alarme et le Log d'événements. Vous pouvez aussi utiliser des critères de recherche pour arranger plus facilement les enregistrements.

9.2.1 Utilisation d'un critère de recherche

1. Choisissez le journal désiré dans le panneau gauche. Dans cet exemple, nous allons utiliser le Log d'accès.
2. En haut de la fenêtre du journal, cliquez sur le bouton **Flèche bas** Condition. Une boîte de dialogue de filtre s'affiche.

3. Entrez ou sélectionnez le critère de filtrage désiré. Par exemple, vous voulez chercher le journal des enregistrements correspondant aux critères « Accès accordé », Numéro de badge « 100012 », Porte de devant (Dir d'entrée) et entre le 20 Août et le 26 Août. La fenêtre de résultat obtenue ressemblera à :

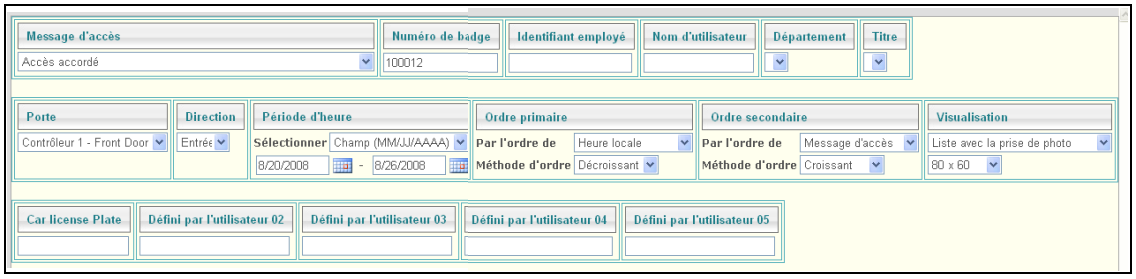


Figure 9-5

4. Dans les listes déroulantes Ordre primaire et Ordre secondaire, choisissez comment les résultats de la recherche doivent être triés et affichés sur l'écran.
5. Dans la liste déroulante Affichage, sélectionnez **Liste** pour afficher une liste des résultats de la recherche, **Liste avec la prise de photo** pour afficher une liste des résultats avec les images vidéo associées, ou **Vérification de la prise de photo** pour afficher les images vidéo trouvées avec les photos des utilisateurs de badge pour vous permettre de vérifier si l'utilisateur et la personne sont les mêmes. La taille de l'image et de la photo peut être sélectionnée.
6. Cliquez sur le bouton **Soumettre** pour commencer la recherche du journal.

9.2.2 Icônes de la fenêtre de journal

Les icônes de la fenêtre de journal peuvent afficher des informations détaillées sur cette catégorie. Cliquez sur une icône pour afficher les détails.

: Pour afficher les informations du badge.

: Indique qu'une séquance vidéo enregistré existe.

: Indique qu'une image vidéo est disponible.

Remarque : Vous pouvez relire la vidéo seulement lorsque le Service ViewLog à distance dans le Serveur du centre de contrôle est activé sur l'enregistreur. Et la fonction ViewLog à distance est activée sur le Serveur vidéo ou sur le Compact DVR.

9.2.3 Exporter des journaux

Vous pouvez télécharger les journaux du ASManager connecté sur l'ordinateur dans trois formats : **.txt**, **.htm** et **.xls**.

1. Utilisez la liste déroulante Exporter vers et choisissez le format de fichier **TXT**, **HTML** ou **Excel**.
2. Utilisez la liste déroulante suivante pour sélectionner **Cette page** pour enregistrer la page actuelle du journal ou **Tout** pour enregistrer tous les journaux.
3. Cliquez sur **Exporter** pour télécharger les journaux.

9.2.4 Définir des colonnes

Vous pouvez définir les colonnes affichées pour chaque type de journal.

1. Dans la barre de menu de ASManager, cliquez sur **Outils** et choisissez **Champ ASWeb**. La boîte de dialogue suivante s'affiche.

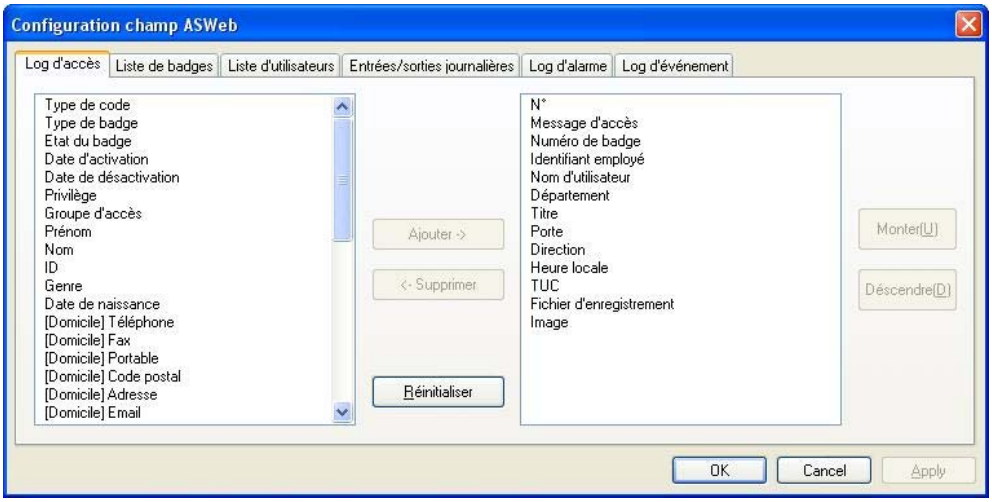


Figure 9-6

2. Cliquez sur le bouton du journal désiré, par ex. Journal d'accès. Les colonnes par défaut sont affichées à droite. Utilisez ensuite **Ajouter** ou **Supprimer** pour définir les colonnes du journal.

   Par exemple, nous avons ajoutés un champ défini par l'utilisateur ″Plaque immatriculation de véhicule (Car License Plate) ″ dans le Journal d'accès. La fenêtre de ASWeb ressemblera donc à :

Figure 9-7

Chapitre 10 Guide de dépannage

Q1 : ASManager n'arrive pas à se connecter au Contrôleur AS200 sur Internet.

Ce problème peut être causé par plusieurs raisons, par exemple un conflit d'adresse IP, une configuration incorrecte de connexion et une panne du réseau. La solution décrite ci-dessous est pour assigner une adresse IP fixe à ASManager et au Contrôleur AS200, respectivement. Ceci permet de déterminer si le problème est causé par des périphériques défectueux et une configuration incorrecte du réseau.

1. Déconnectez le hub ou le commutateur, qui connecte ASManager et le Contrôleur AS200, du réseau.
2. Choisissez une adresse IP fixe pour ASManager qui n'est PAS utilisée par un autre périphérique, par ex. 192.168.0.154.

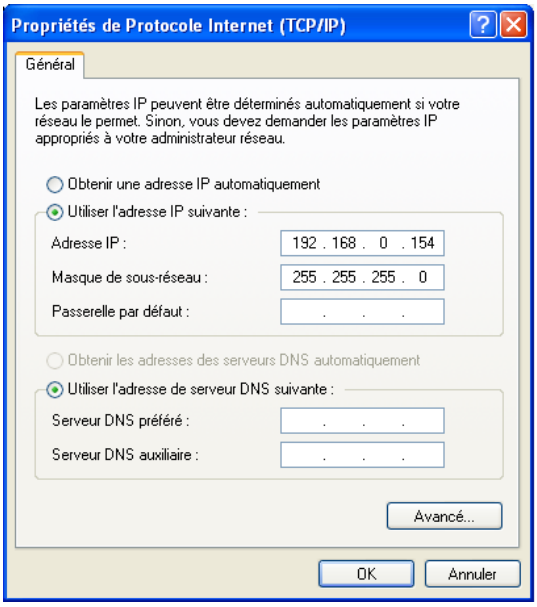

Propriétés de Protocole Internet (TCP/IP)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP :
192 . 168 . 0 . 154
Masque de sous-réseau :
255 . 255 . 255 . 0
Passerelle par défaut :
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :
Avancé...
OK
Annuler

Figure 10-1

3. Réinitialisez le module Contrôleur AS200 et le module Ethernet sur les réglages par défaut.
   a. Branchez l'ASKeypad sur le Contrôleur AS200.
   b. Enlevez le couvercle du cavalier du cavalier **Défaut** à 2 fiches.
   c. Appuyez sur le bouton **Réinitialiser(Reset)**.
   d. Remettez le couvercle du cavalier du cavalier **Défaut** à 2 fiches.
   e. Pour réinitialiser le module Ethernet, appuyez pendant 6 secondes sur le bouton **Defaut EN**.
4. Ouvrez le navigateur Internet et entrez l'adresse IP par défaut du Contrôleur AS200 : http://192.168.0.100

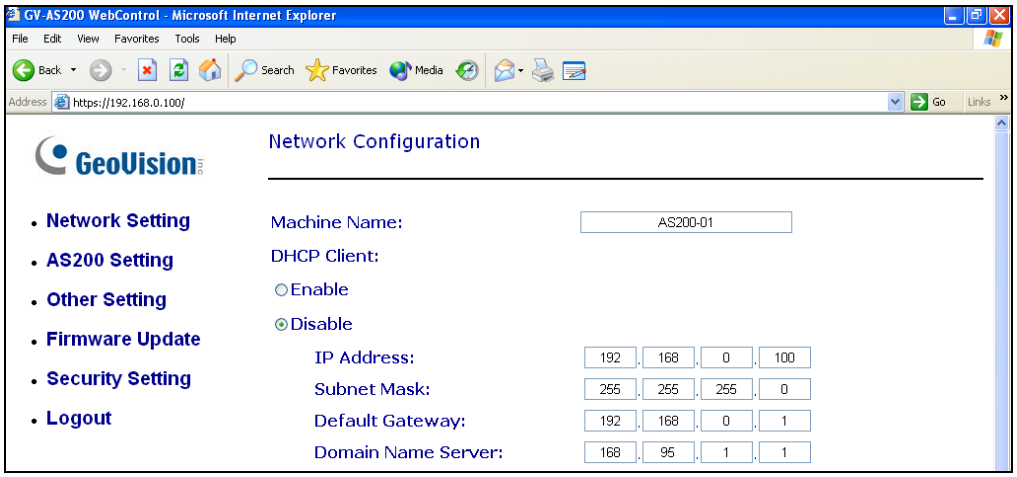


Figure 10-2

5. Dans le champ de l'adresse IP, entrez une adresse IP fixe pour le Contrôleur AS200 qui n'est PAS utilisée par un autre périphérique, par ex. 192.168.0.XXX.
6. Dans le ASManager, entrez les réglages suivants :

   Identifiant contrôleur : 1

   Réseau : TCP/IP

   IP : 192.168.0.XXX

   Port : 4000

   Utilisateur : admin

   Mot de passe : 1234

   Clé de cryptage : 12345678

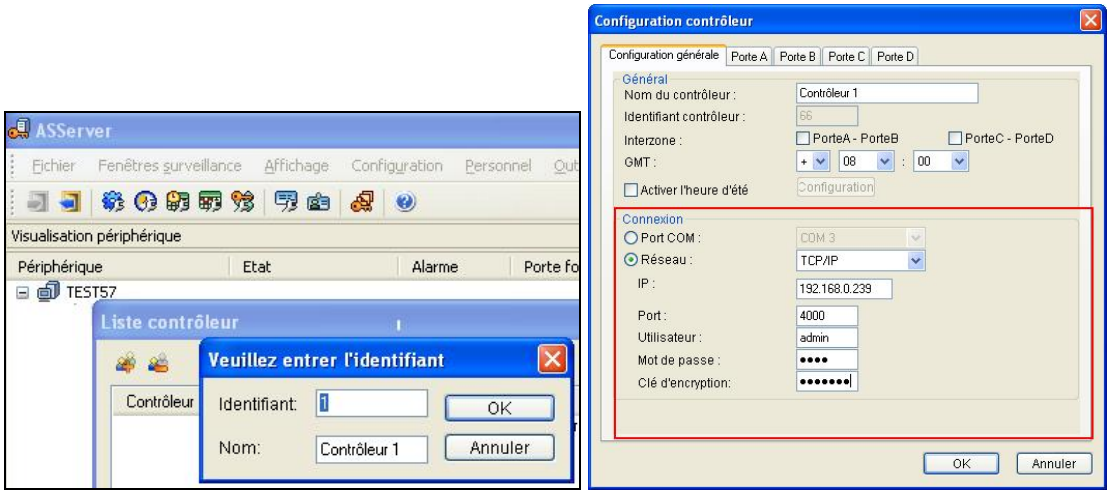


Figure 10-3

7. La connexion entre le ASManager et le Contrôleur AS200 devrait s'établir, et l'icône de connexion devrait apparaître. Si vous êtes déconnecté lorsque vous connectez le hub ou le commutateur au réseau, alors il s'agit d'un problème est un problème de réseau. Veuillez contacter votre administrateur réseau.

Q2 : La connexion entre le ASManager et le Contrôleur AS200 est interrompue.

Ceci peut être causé par un conflit d'adresse IP. Suivez les étapes suivantes pour résoudre ce problème :

1. Déconnectez le hub ou le commutateur, qui connecte le ASManager et le Contrôleur AS200, du réseau.
2. Ouvrez la fenêtre **Invite de commande**. Dans la version classique de Windows par exemple, cliquez sur **Démarrer**, choisissez **Accessoires** et cliquez sur **Invite de commande**.
3. Entrez **arp –d** et appuyez sur **Entrer**.

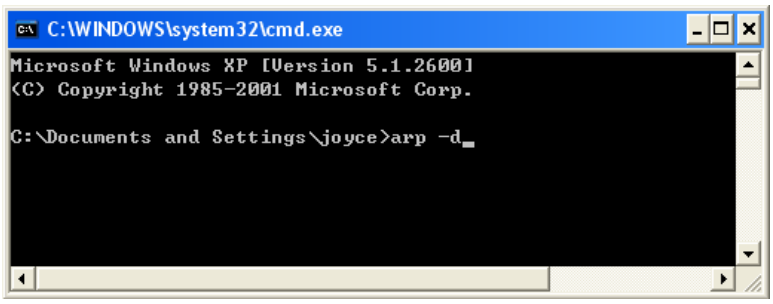


Figure 10-4

4. Choisissez une adresse IP fixe pour le ASManager qui n'est PAS utilisée par un autre périphérique. Voir Figure 10-1.
5. Ouvrez le navigateur Internet et entrez l'adresse IP assignée du Contrôleur AS200. La page de configuration du réseau s'affiche. Voir Figure 10-2.
6. Dans le champ de l'adresse IP, entrez une adresse IP fixe pour le Contrôleur AS200 qui n'est PAS utilisée par un autre périphérique, par ex. 192.168.0.XXX.
7. Dans le ASManager, entrez les réglages suivants : Voir Figure 10-3.

   Identifiant contrôleur : 1

   Réseau : TCP/IP

   IP : 192.168.0.XXX

   Port : 4000

   Utilisateur : admin

Mot de passe : 1234

Clé de cryptage : 12345678

8. La connexion entre le ASManager et le Contrôleur AS200 devrait s'établir, et l'icône de connexion devrait apparaître. Si vous êtes déconnecté lorsque vous connectez le hub ou le commutateur au réseau, alors il s'agit d'un problème est un problème de réseau. Veuillez contacter votre administrateur réseau.

Q3 : ASManager ne reçoit pas les messages de badge mais le lecteur accepte le badge lorsque la connexion entre le ASManager et le Contrôleur AS200 est correctement établie.

Ceci peut être causé par un problème de mémoire dans le Contrôleur AS200. Réinitialisez le module Contrôleur AS200 et le module Ethernet sur les réglages par défaut. Voir l'Etape 3 de la Question 1.

Q4 : Le ASManager ne peut pas obtenir la vidéo de l'enregistreur pour la lecture.

1. Vérifiez que le **Service ViewLog à distance** sur le **Serveur du centre de contrôle** est activé.
2. Vérifiez que l'heure sur le ASManager et l'enregistreur est la même.
3. Vérifiez que le fichier de l'événement que vous voulez lire a été complètement créé par l'enregistreur. Par exemple, la durée de chaque enregistrement d'un événement par l'enregistreur est réglée sur 5 minutes. L'événement désiré de 5 minutes doit être affiché dans la Liste des événements ViewLog pour que vous puissiez accéder au fichier de l'événement pour la lecture.

Q5 : Après avoir ajouté un badge en le glissant dans le lecteur, le message « *Accès refusé – badge invalide* » s'affiche toujours.

(Pour plus de détails sur comment faire pour ajouter un badge, voir Etape 1, *4.3.1 Ajouter un seul badge.)*

Le format du badge est peut-être incompatible avec le Contrôleur AS200. Vérifiez que le format de votre lecteur de carte est un périphérique Wiegand de 26-40 bits. Autrement envoyez-nous les informations du format du badge pour que nous puissions personnaliser ce format pour vous.

Q6 : Le ASManager ne reçoit pas les messages de badge du GV-Reader connecté au Contrôleur AS200 via l'interface RS-485.

1. Vérifiez que le GV-Reader est correctement branché sur le Contrôleur AS200 et que le Commutateur 4 est réglé sur OFF. Voir « Connexion au Contrôleur AS200 via l'interface RS-485 », *Guide d'installation du GV-Reader*.
2. Vérifiez que l'identifiant du GV-Reader est réglé sur le Contrôleur AS200.
   a. Branchez l'ASKeypad sur le Contrôleur AS200.
   b. Appuyez sur un bouton du clavier numérique, choisissez **Régler paramètres (Set Parameter)** et appuyez sur le bouton ENT YES.
   c. Entrez le mot de passe par défaut **1234** et choisissez **Régler identifiant du GV-Reader (Set GV-Reader ID)** en utilisant les boutons flèche de navigation HAUT(UP) et BAS (Down).
   d. Changez l'identifiant 0 du GV-Reader sur **Wiegand étendu (Extended Wiegand).**

Q7 : Comment faire pour ouvrir automatiquement toutes les portes lorsqu'un incendie est détecté?

Suivez les étapes suivantes pour connecter le Contrôleur AS200 et configurer le ASManager :

1. Raccordez les deux fiches Incendie de la Porte A et de la Porte B (indiqué par la ligne Rouge).
2. Raccordez les deux fiches GND de la Porte A et de la Porte B (indiqué par la ligne Noire).
3. Raccordez le détecteur d'incendie aux fiches Incendie et GND de la Porte A (indiqué par les lignes Vertes).
4. Raccordez le détecteur d'incendie aux fiches Incendie et GND de la Porte B (indiqué par les lignes Violettes).

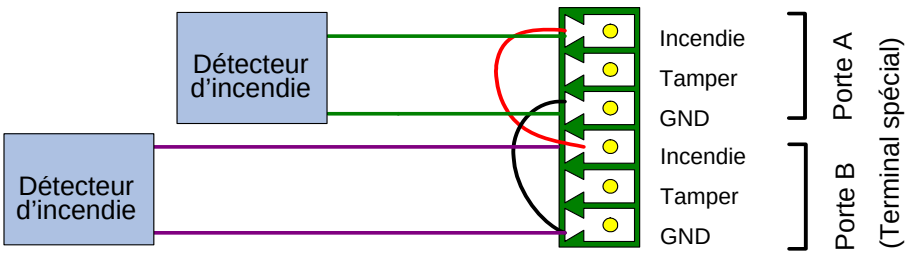


Figure 10-5

5. Dans la boîte de dialogue Configuration contrôleur, cliquez sur l'onglet **Porte A** et **Porte B**, respectivement, et choisissez **Déverrouiller la porte** dans l'option Action en cas d'incendie.

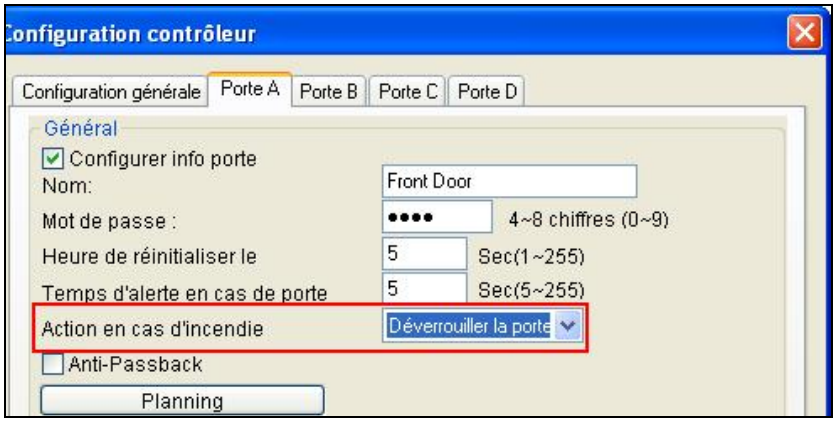


Figure 10-6

Q8 : Où puis-je trouver plus d'aide ?

Pour plus de détails, visitez http://www.geovision.com.tw

Ecrivez nous à support@geovision.com.tw

Appendice

A. Appareils IP compatibles

No.	Modèle	No.	Modèle
1	Caméra GV-IP	33	JVC VN-C625U
2	Serveur GV-Video	34	JVC VN-C655U
3	Enregistreur GV-Compact	35	Mobotix M12
4	Arecont AV-1300	36	SONY SNC-CS10
5	Arecont AV-2100	37	SONY SNC-CS11
6	Arecont AV-3100	38	SONY SNC-CS50N
7	Arecont AV-5100	39	SONY SNC-CS50P
8	AXIS 206	40	SONY SNC-DF40N
9	AXIS 207 / AXIS 207W	41	SONY SNC-DF40P
10	AXIS 207MW	42	SONY SNC-DF50N
11	AXIS 210	43	SONY SNC-DF50P
12	AXIS 211	44	SONY SNC-DF70N
13	AXIS 211A	45	SONY SNC-DF70P
14	AXIS 212 PTZ	46	SONY SNC-DF80N
15	AXIS 213 PTZ	47	SONY SNC-DF80P
16	AXIS 214 PTZ	48	SONY SNC-P1
17	AXIS 216FD / AXIS 216FD-V	49	SONY SNC-P5
18	AXIS 221	50	SONY SNC-RX550N
19	AXIS 223M	51	SONY SNC-RX550P
20	AXIS 225FD	52	SONY SNC-RZ25N
21	AXIS 231D+	53	SONY SNC-RZ25P
22	AXIS 232D+	54	SONY SNC-RZ50N
23	AXIS 233D	55	SONY SNC-RZ50P
24	IQEye 301	56	Panasonic BB-HCM110
25	IQEye 302	57	Panasonic BB-HCM311
26	IQEye 510	58	Panasonic BB-HCM331
27	IQEye 511	59	Panasonic BB-HCM371
28	IQEye 701	60	Panasonic BB-HCM381
29	IQEye 702	61	Panasonic BB-HCM403
30	JVC VN-C20U	62	Panasonic BB-HCE481A
31	JVC VN-C205U	63	Panasonic BL-C10
32	JVC VN-C215U	64	Panasonic BL-C30

B. Notifications d'événements

- **Evénements « d'alarme »**

Type	Description
Porte forcée	La porte <nom> a été ouverte avec force.
Contrainte	La fonction Contrainte a été déclenchée. Voir « Contrainte » dans *1.2 Concepts*.
Vandalisme	Les entrées vandalisées ont été déclenchées. Pour la configuration matérielle, voir *3.2 Connexion des entrées* dans le Guide d'installation matérielle du contrôleur GV-AS200. Pour les réglages du logiciel, voir Etape 5 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Alarme incendie	Les entrées d'incendie ont été déclenchées. Pour la configuration matérielle, voir *3.2 Connexion des entrées* dans le Guide d'installation matérielle du contrôleur GV-AS200. Pour les réglages du logiciel, voir Etape 5 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Restant ouverte	La porte <nom> est restée ouverte pendant une période de temps spécifiée. Pour les réglages du logiciel, voir Etape 5 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte.*
Accès refusé	L'accès a été refusé.

- **Evénements « d'accès »**

Type	Description
Accès accordé	L'accès pour <nom> d'utilisateur de badge et le badge <Numéro> a été permis.
Accès refusé : badge invalide	L'accès a été refusé car un badge inconnu a été utilisé.
Accès refusé : badge bloqué	L'accès a été refusé car le badge <Numéro> a été suspendu.
Accès refusé : mauvais PIN	L'accès a été refusé car le numéro PIN entré est incorrect.
Accès refusé : badge expiré	L'accès a été refusé car le badge <Numéro> a expiré.
Accès refusé : horaire invalide	L'accès a été refusé car l'accès pour l'utilisateur n'est pas dans un planning programmé.
Accès refusé : mauvaise porte	L'accès a été refusé car l'utilisateur a utilisé une porte incorrecte.

Accès refusé : APB (Double entrées)	L'accès a été refusé car la fonction Anti-Passback a été activée. Le badge <Numéro> a été utilisé pour des entrées successives, sans sortie, dans une zone sécurisée. Voir la fonction « Anti-Passback » dans Etape 2 dans la section 4.2.2 de l'*Etape 2: Configurer une porte.*
Accès refusé : APB (Aucune entrée)	L'accès a été refusé car la fonction Anti-Passback a été activée. Le badge <Numéro> a été utilisé pour sortir, sans entrée, dans une zone sécurisée.
Accès refusé : APB (Aucune sortie)	L'accès a été refusé car la fonction Anti-Passback a été activée. Le badge <Numéro> a été utilisé pour entrer, sans sortie, dans une zone sécurisée.
Accès refusé : badge inconnu	L'accès a été refusé car le format du badge est incompatible.
Accès refusé : heure de début invalide	L'accès a été refusé car le badge <Numéro> n'est pas actif.
Accès refusé : la porte précédente est toujours ouverte (Interlock)	L'accès a été refusé car la fonction Verrouillage a été activée. La porte d'entrée a été laissée déverrouillée. Voir la fonction « Verrouillage » dans Etape 5 dans la section 4.2.1 de l'*Etape 1: Configurer un contrôleur de porte*.

- **Evénement « d'événement »**

Type	Description
Porte forcée	La porte <nom> a été ouverte avec force.
Contrainte	La fonction Contrainte a été déclenchée. Voir « Contrainte » dans *1.2 Concepts*.
Vandalisme	Les entrées vandalisées ont été déclenchées. Pour la configuration matérielle, voir *3.2 Connexion des entrées* dans le Guide d'installation matérielle du contrôleur GV-AS200. Pour les réglages du logiciel, voir Etape 5 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte.*
Alarme incendie	Les entrées d'incendie ont été déclenchées. Pour la configuration matérielle, voir *3.2 Connexion des entrées* dans le Guide d'installation matérielle du contrôleur GV-AS200. Pour les réglages du logiciel, voir Etape 5 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Restant ouverte	La porte <nom> est restée ouverte pendant une période de temps spécifiée. Voir Etape 2 et 5 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte.*

Accès refusé	L'accès a été refusé.
Alarme restauré	Les sons d'alarme ont été annulés.
Porte forcée - restauré	L'alarme Ouverture forcée a été annulée.
Contrainte restauré	L'alarme Contrainte a été annulée.
Vandalisme restauré	L'alarme vandalisée a été annulée.
Alarme incendie restauré	L'alarme d'incendie a été annulée.
Restant ouverte restauré	L'alarme Restée ouverte a été annulée.
Echec à la restauration d'alarme	Echec d'annulation des sons d'alarme.
Echec à la restauration de l'événement porte forcée	Echec d'annulation d'alarme Ouverture forcée.
Echec à la restauration de l'événement contrainte	Echec d'annulation d'alarme Contrainte.
Echec à la restauration de l'événement vandalisme – aucun événement présent	Echec d'annulation d'alarme vandalisée.
Echec à la restauration de l'événement alarme ncendie – aucun événement présent	Echec d'annulation d'alarme d'incendie.
Echec à la restauration de l'événement restant ouverte	Echec d'annulation de l'alarme Restée ouverte.
Echec à la restauration de l'événement accès refusé	Echec d'annulation d'alarme Accès refusé.
Echec à la restauration de l'événement vandalisé – état E/S indéterminé	Echec d'annulation d'alarme vandalisée car les entrées vandalisées sont toujours déclenchées.
Echec à la restauration de l'événement incendie – état E/S indéterminé	Echec d'annulation d'alarme d'incendie car les entrées Incendie sont toujours déclenchées.
Porte ouverte	La porte <nom> est ouverte.
Porte fermée	La porte <nom> est fermée.
Déverrouillage porte/portail	La porte <nom> est déverrouillée.
Vérrouillage porte/portail	La porte <nom> est verrouillée.
Mode double présentation - activé	La règle deux personnes A/B est active lorsque le Badge <numéro> est utilisé.
Mode double présentation - confirmé	La règle deux personnes A/B est confirmée lorsque le Badge <nom> est utilisé après l'autre badge AB.
Mode double présentation - désactivé	La règle deux personnes A/B est désactivée lorsque le Badge <nom> est utilisé successivement ou lorsque l'autre badge AB n'est pas utilisé dans les 20 secondes.
Confirmation du code clavier numérique	Dans le mode Badge ou Commun, le mot de passe entré est correct.

Erreur de code clavier numérique	Dans le mode Badge ou Commun, le mot de passe entré est in correct.
Mode accès ouverte	La porte <nom> est en mode Déclenchement. Voir Etape 4 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Mode badge ou clavier numérique	La porte <nom> est en mode Badge ou Commun. Voir Etape 4 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Mode Badge et code PIN	La porte <nom> est en mode Badge et code PIN. Voir Etape 4 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Mode badge	La porte <nom> est en mode Badge. Voir Etape 4 dans la section 4.2.2 de l'*Etape 2 : Configurer une porte*.
Mode déverrouillage en cas d'incendie	La porte <nom> est déverrouillée lorsque les entrées d'incendie sont déclenchées. Voir « Action d'incendie » dans l'Etape 2 dans la section 4.2.2 de *Etape 2 : Configurer une porte*.
Mode verrouillage en cas d'incendie	La porte <nom> est verrouillée lorsque les entrées d'incendie sont déclenchées. Voir « Action d'incendie » dans l'Etape 2 dans la section 4.2.2 de *Etape 2 : Configurer une porte*.
Forcer déverrouillage à distance	La porte <nom> est déverrouillée à distance avec le contrôle de ASManager ou le serveur ASRemote.
Forcer verrouillage à distance	La porte <nom> est verrouillée à distance avec le contrôle de ASManager ou le serveur ASRemote.
Désactiver verrouillage à distance	L'événement « Forcer déverrouillage à distance » ou « Forcer déverrouillage à distance » est annulé.
Forcer déverrouillage en local	La porte <nom> est déverrouillée sur le site du Contrôleur de porte.
Forcer verrouillage en local	La porte <nom> est verrouillée sur le site du Contrôleur de porte.
Désactiver verrouillage enlocal	L'événement « Forcer déverrouillage local » ou « Forcer déverrouillage local » est annulé.
Réinitialiser	Le contrôleur de porte <nom> est réinitialisé.

C. Symboles d’alerte Email et SMS

Icône	Description
	%M (Message) : contient le message d’alerte associé.
	%T (Contrôleur) : contient le nom du contrôleur de la porte.
	%D (Porte) : contient le nom de la porte déclenchée.
	%L (Heure locale) : contient l’heure locale.
	%U (TUC) : contient l’heure UTC.
	%N (Numéro de badge) : contient le numéro du badge.
	%H (Nom de l’utilisateur du badge) : contient le nom de l’utilisateur du badge.
	%G (Genre) : contient le sexe de l’utilisateur du badge.
	%E (Identifiant employé) : contient l’ID de l’employé.
	%Y (Société) : contient le nom de la compagnie.
	%P (Département) : contient le nom du département.
	%F (Bureau) : contient le nom du bureau.
	%C (Photo) : contient la photo de l’utilisateur du badge.
	%S (Prise de photo) : contient une image.